

IKARUS gateway.security

Benutzerhandbuch


IKARUS
gateway.security



Inhaltsverzeichnis


IKARUS
gateway.security


IKARUS
gateway.security


IKARUS
gateway.security



Abbildungsverzeichnis


IKARUS
gateway.security


IKARUS
gateway.security



Tabellenverzeichnis


IKARUS
gateway.security



1 Allgemeines zu IKARUS gateway.security

1.1 Einleitung / Bedrohungsbild

Heutzutage ist ein Unternehmen ohne Datenaustausch über das Internet am Markt praktisch chancenlos. Dabei ist es egal, ob es sich um ein KMU, einen weltweiten Konzern, Bildungs- oder andere öffentliche Einrichtungen oder auch ISPs handelt – fast jeder ist bei seinem täglichen Tun mit dem Medium Internet auf das Funktionieren des Selbigen angewiesen.

Dies führt dazu, dass die Verfügbarkeit des World Wide Web fälschlicherweise als Selbstverständlichkeit angesehen wird. Jedoch wird nicht selten darauf vergessen, dass die dabei am häufigsten eingesetzten Werkzeuge, nämlich E-Mail und Internet, praktisch das Einfallstor für den Großteil der Angriffe von Malware sind. Diese Attacken werden in den nächsten Jahren noch stärker zunehmen und raffinierter werden.

Viel schlimmer ist jedoch die Tatsache, dass Unternehmen oft selbst unbewusst zur Verbreitung von gefährlichem Schadcode beitragen, indem sie ihren Mitarbeiten die Möglichkeit bieten, ungehindert verseuchte Internetseiten anzusurfen, Dateien aus dem Internet zu laden bzw. aus dem Unternehmen in das Internet zu versenden. Die Auswirkungen auf die Netzwerkstrukturen sind oftmals dramatisch: Server werden durch Unmengen von SPAM und dem enormen Datenvolumen ausgebremst. Damit sind wertvolle Daten einem erheblichen Risiko ausgesetzt, kostbare Arbeitszeit der Mitarbeiter wird vergeudet und nebenbei entstehen dadurch vermeidbare Kosten.

Nur ein effektiver Gateway-Schutz kann dazu beitragen, die Effizienz Ihrer Kommunikation über das Internet zu steigern. Ohne diesen Schutz sind Sie den Angriffen aus dem Web hoffnungslos ausgeliefert.

1.2 Produkt Details

IKARUS gateway.security ist eine Software-Content-Security-Lösung und kann mit minimalem Aufwand sowohl im internen Netzwerk als auch bereits auf Gateway-Level eingesetzt werden. Diese Lösung schützt bereits kleine Unternehmen mit wenigen Nutzern als auch Unternehmen mit mehreren tausend Nutzern.

Einer Kombination mit jeder beliebigen Firewall steht aufgrund der uneingeschränkten Kompatibilität nichts im Wege. Die Installationspakete sind sowohl für Microsoft Windows als auch für Linux (als RPM Paket) erhältlich. Eine der innovativsten Entwicklungen stellt die Ausprägung von **IKARUS gateway.security** für Microsoft Internet Security & Acceleration (ISA) Server bzw. Microsoft Threat Management Gateway (TMG) dar, bei der die Möglichkeit geschaffen wurde, die umfassenden Funktionen der Content-Security-Lösung aus dem Hause **IKARUS** transparent mit dem MS ISA/TMG Server zu kombinieren.

Alle Ausprägungen von **IKARUS gateway.security** sind auch als Komplettlösung auf SecureGUARD Appliances verfügbar.

1.3 Funktionen

Die vollständige und aktuelle Liste der Funktionen von **IKARUS gateway.security** entnehmen Sie bitte dem Online-Auftritt von **IKARUS** unter www.ikarus.at.

Hier ein Auszug der Funktionen:



- Integrierte AntiVirus **IKARUS** ScanEngine
- AntiVirus Schutz für Web-Protokolle (HTTP, FTP over HTTP, FTP) und Mail-Protokolle (SMTP, IMAP, POP3, NNTP)
- AntiSPAM: **IKARUS** AntiSPAM Engine für Mail-Protokolle (SMTP, IMAP, POP3, NNTP)
- Greylisting Support, SPF Support (SMTP)
- TLS Support (SMTP)
- Einfache Erstellung von Berechtigungsprofilen mittels URL-, File- und Content-Type-Listen
- Zugriffssteuerung mittels IP-Adress-Gruppen
- IPv6-Unterstützung für ausgehende Verbindungen
- Authentifizierung mittels Basic Proxy Authentication, LDAP Authentication und NTLM/Kerberos Authentication (letzteres nur unter Windows)
- Inkrementelles automatisiertes Update (alle 10 Minuten) für Virendatenbank, AntiSPAM-Datenbank, URL-Filter-Datenbank, **IKARUS** ScanEngine sowie IKARUS AntiSPAM Engine
- Erstellung unterschiedlicher administrativer Berechtigungsstufen
- Activity Monitor (**IKARUS gateway.security Configuration Center**)
- Umfassende Log-Information aller Aktivitäten
- Reporting-Funktionalität zur übersichtlichen und automatisiert versendbaren Auswertung der gesammelten Daten
- Installationspakete für Microsoft Windows und Linux
- Ausprägung für Microsoft ISA/TMG
- Integration in bestehende Managementoberfläche, anwendbares Regelset auf bestehende ISA/TMG-Regeln, volltransparente Antiviren- und URL-Filter-Integration
- Vorinstalliert als Komplettlösung auf SecureGUARD Appliances erhältlich



2 Installation

2.1 Voraussetzungen

Die Installation von **IKARUS gateway.security** bedarf einiger vorbereitender Maßnahmen.

- Um die Installation am System durchführen zu können, braucht der Benutzer administrative Rechte.
- Systemzeit muss korrekt sein.
- Abgeschlossene Netzwerkkonfiguration des Betriebssystems: IP-Adresse, Routing (Default-Gateway), DNS Auflösung
- Ausreichend Speicherplatz
- Sind die Standard-Ports von **IKARUS gateway.security** frei? TCP 8080, TCP 2100, TCP 15639
- Firewall-Freischaltung vom System nach außen (HTTP, HTTPS, POP3, IMAP, NNTP, SMTP)
- Firewall-Freischaltung auf das System (Management Port TCP 15639, Web Proxy Port TCP 8080)
- Setup Datei für **IKARUS gateway.security** (Architektur beachten – 32bit oder 64bit)
- Lizenz für **IKARUS gateway.security** (DEMO-Lizenz oder vollwertige Kauf-Lizenz)

2.2 Installation auf Microsoft Windows

Die Installation unter Windows gestaltet sich sehr einfach. Es wird nach einem Doppelklick das Service **IKARUS gateway.security** am System installiert. Folgen Sie einfach den Anweisungen des Setups.

Hinweis: Es wird empfohlen, soweit möglich die vorgegebenen Einstellungen zu übernehmen.

Im Zuge der Installation können Sie Ihre Lizenz für **IKARUS gateway.security** einspielen. Dies können Sie aber per **IKARUS gateway.security Configuration Center** später auch noch nachholen.

Dasselbe gilt für die Installation des **IKARUS gateway.security Configuration Center**.

2.3 Installation auf Linux

Für die Installation von **IKARUS gateway.security** unter Linux werden sowohl RPM als auch DEB-Pakete zur Verfügung gestellt. Diese sind jeweils in einer 32-bit und 64-bit Variante erhältlich.

```
# rpm -ivh IKARUSSecurityProxy-3.26.3rh5.x86_64.rpm
```

```
# dpkg -i IKARUSSecurityProxy-3.26.3_amd64.deb
```



2.4 Lizenzierung

Während der Installation unter Windows werden Sie aufgefordert die Lizenz hinzuzufügen. Unter Linux können Sie dies nach der Installation über die Kommando-Zeile durchführen.

Bsp. 64bit Linux:

```
# cd /opt/securityproxy/bin
# ./securityproxy_l64 -importlicense <licensefile>
```

2.5 Stoppen und Starten

2.5.1 Unter Microsoft Windows

Das Service **securityproxy** wird unter den am System installierten Services aufgelistet. Es kann wie jedes andere Service über die administrativen Tools angehalten und gestartet werden.

2.5.2 Unter Linux

Das Service **securityproxy** wird am Linux Betriebssystem in den entsprechenden *run-levels* registriert. Ein Anhalten und Starten erfolgt über ein Start-Skript, wie unter Linux üblich:

```
# /etc/init.d/securityproxy stop
# /etc/init.d/securityproxy start
```

oder

```
# /etc/init.d/securityproxy restart
```

2.6 Nutzung von IKARUS gateway.security

Nach der Installation kann **IKARUS gateway.security** sofort verwendet werden. Es muss lediglich am Web-Client (Microsoft Internet Explorer, Mozilla Firefox, Opera, usw.) ein Proxy definiert werden. Dazu wird der DNS Name oder die IP-Adresse des Systems benötigt und das Standard TCP Port 8080.



3 Konfiguration

3.1 Bearbeitungsmenü

Über das Bearbeitungsmenü können Sie diverse generelle Einstellungen für **IKARUS gateway.security** vornehmen.

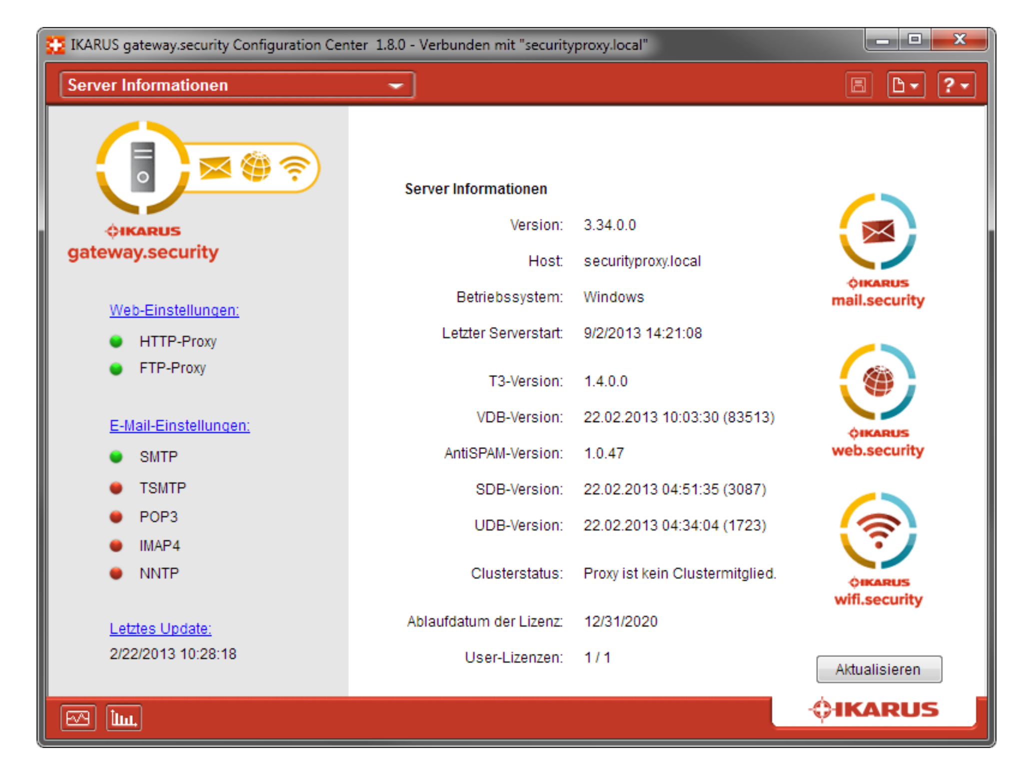


Abbildung 1: Bearbeitungsmenü

Wert	Beschreibung
Änderungen speichern	An der Konfiguration vorgenommene Änderungen werden gespeichert und an **IKARUS gateway.security** übertragen. Sollte die vorgenommene Änderung einen Neustart von **IKARUS gateway.security** notwendig machen, so werden Sie in einem Dialog darüber informiert.
Änderungen verwerfen	An der Konfiguration vorgenommene und noch nicht gespeicherte Änderungen werden rückgängig gemacht. Die Konfiguration wird von **IKARUS gateway.security** neu geholt.
Konfigurationsdatei exportieren	Diese Option erlaubt Ihnen, die aktuelle Konfiguration von **IKARUS gateway.security** als Textdatei an einem von Ihnen bestimmten Ort zu speichern.
Konfigurationsdatei importieren	Über "Konfigurationsdatei importieren" sind Sie in der Lage, eine extern gespeicherte Konfigurationsdatei nach **IKARUS gateway.security** zu importieren.
Standardkonfiguration wiederherstellen	Diese Option erlaubt Ihnen die Wiederherstellung der Voreinstellungen von **IKARUS gateway.security** – also jenes Zustandes, mit dem **IKARUS gateway.security** installiert wurde. Achtung: durch die Auswahl dieser Option werden sämtliche vorher vorgenommenen Einstellungen verworfen und überschrieben.
IKARUS gateway.security-Service neu starten	Das Service kann manuell neu gestartet werden, um z.B. Änderungen an der Konfiguration zu übernehmen.
Ausloggen	Diese Option erlaubt Ihnen das Ausloggen aus dem **IKARUS gateway.security Configuration Center**. Das **IKARUS gateway.security Configuration Center** schließt sich und Sie befinden sich wieder in der Anmeldemaske.
Speichern und Beenden	An der Konfiguration vorgenommene Änderungen werden gespeichert und an **IKARUS gateway.security** übertragen. Danach wird das **IKARUS gateway.security Configuration Center** beendet. Sollte die vorgenommene Änderung einen Neustart von **IKARUS gateway.security** notwendig machen, so werden Sie in einem Dialog darüber informiert.
Beenden	Mit der Option "Beenden" wird das **IKARUS gateway.security Configuration Center** beendet.

Tabelle 1: Bearbeitungsmenü

3.2 Hilfsmenü

Das Hilfsmenü erlaubt Ihnen, Änderungen – wie z.B. die Anzeigesprache des **IKARUS gateway.security Configuration Centers** – vorzunehmen, die Lizenzen zu verwalten oder Support-Informationen zu speichern.

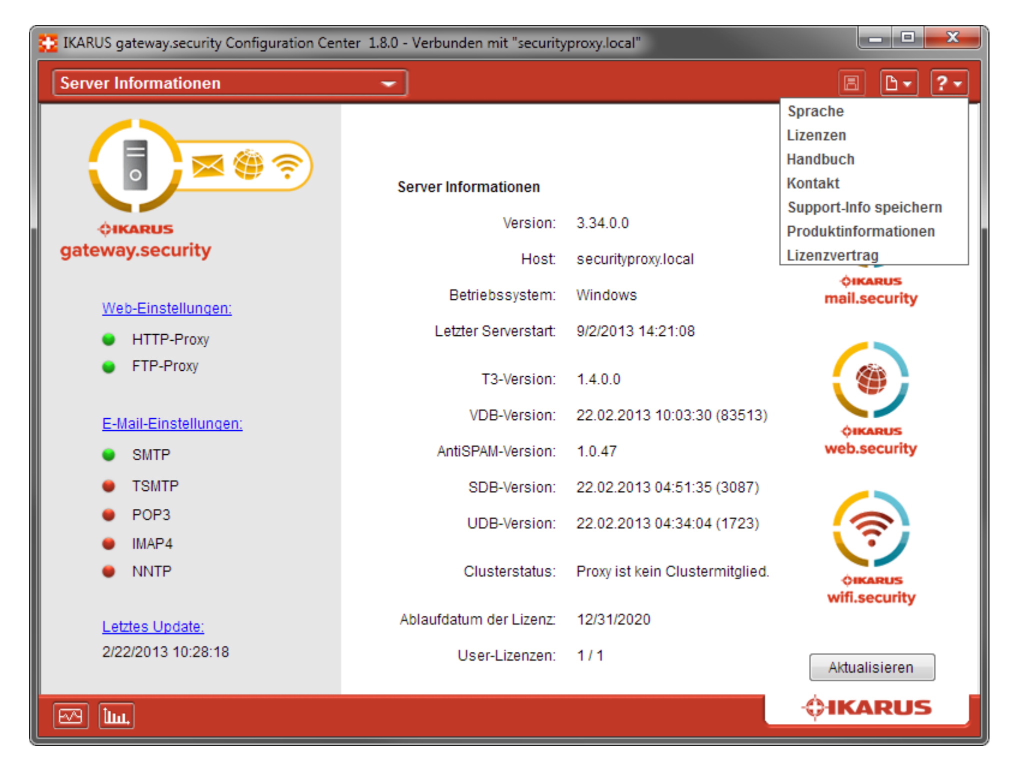


Abbildung 2: Hilfsmenü

Wert	Beschreibung
Sprache	Diese Option erlaubt Ihnen die Änderung der Sprache des **IKARUS gateway.security Configuration Centers**. Zum Zeitpunkt des Verfassens dieses Handbuchs sind Sprachversionen in Englisch, Deutsch und Italienisch verfügbar. Beim Betätigen dieser Option erscheint ein Dialog, in dem Sie die gewünschte Sprache auswählen können. Durch Bestätigen mit dem Button „Annehmen“ werden die Änderungen übernommen. Um das **IKARUS gateway.security Configuration Center** in der gewünschten Sprache anzuzeigen, ist ein Neustart desselben vonnöten.
Lizenzen	Dieser Menüpunkt öffnet einen Dialog, in dem Sie die Lizenzen für **IKARUS gateway.security** verwalten können. Der Dialog listet die für die verwaltete Installation von **IKARUS gateway.security** gespeicherten Lizenzen auf. Mittels des Buttons „Lizenzen bereinigen“ können sie abgelaufene und ungültige Lizenzen entfernen, mittels des Buttons „Lizenz löschen“ können Sie eine in der Übersichtsliste markierte Lizenz entfernen und über den Button „Lizenz hinzufügen“ ist es möglich, eine neue Lizenz zum Proxy hinzuzufügen.
Handbuch	Öffnet das Benutzerhandbuch für **IKARUS gateway.security**.
Kontakt	Zeigt die Kontaktdaten an.
Support-Info speichern	Öffnet einen Dialog, mit dem Sie ein Support-Info-ZIP anlegen können, welche alle wichtigen Informationen (Konfigurationsdatei, Logfiles, Lizenzinformationen und Versionsübersicht) für einen Support-Fall beinhaltet. Dieses können Sie im Bedarfsfall dann an unseren Support senden.
Produktinformationen	Öffnet ein Übersichtsfenster, das die aktuelle Version von **IKARUS gateway.security** angibt.
Lizenzvertrag	Öffnet ein Fenster, welches den Lizenzvertrag für **IKARUS gateway.security** anzeigt.

Tabelle 2: Hilfsmenü

3.3 Serverinformationen

Nach einem erfolgreichen Login wird eine kurze Zusammenfassung des Systems angezeigt. Die Seite „Server Informationen“ ist in 2 Spalten geteilt. Die linke Spalte zeigt die aktivierten und nicht aktivierten **IKARUS gateway.security** Dienste. Die rechte Spalte informiert über folgende Werte:

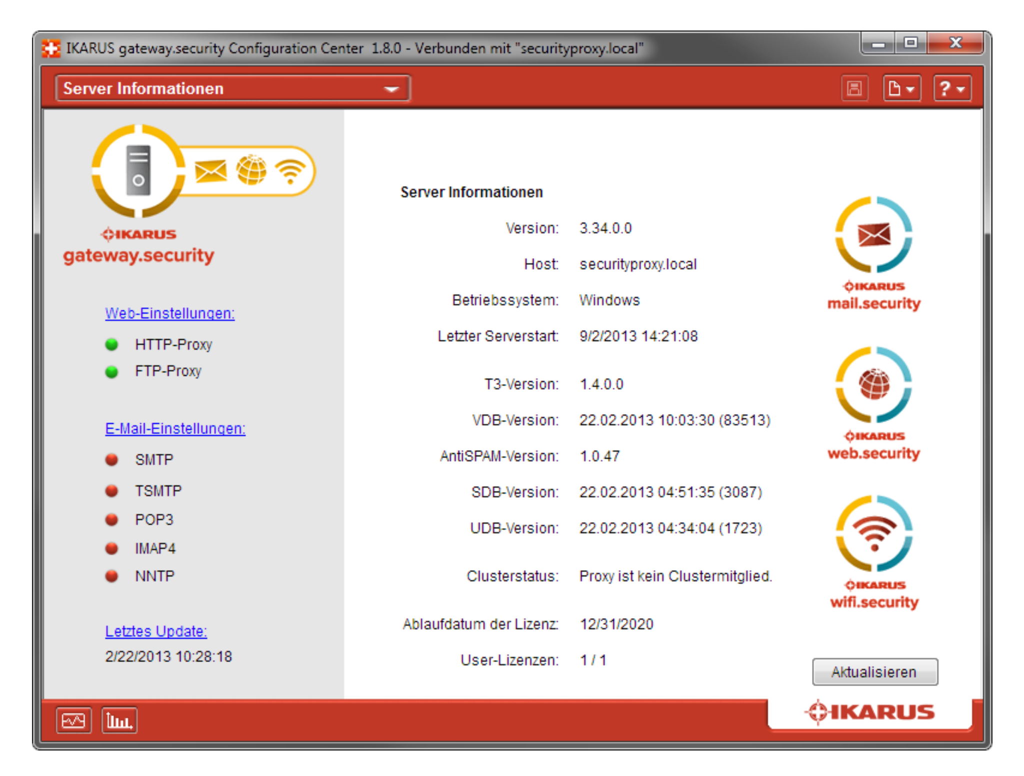


Abbildung 3: Serverinformationen

Wert	Beschreibung
Version	Zeigt die Version von **IKARUS gateway.security**
Host	Der Name des Servers auf dem **IKARUS gateway.security** installiert ist
Betriebssystem	Betriebssystem des Servers auf dem **IKARUS gateway.security** installiert ist
Letzter Serverstart	Zeitpunkt des letzten Starts von **IKARUS gateway.security**
T3-Version	Version der IKARUS Scan Engine
VDB-Version	Version der IKARUS Virendatenbank
Antispam-Version	Version des IKARUS Antispam Plugins
SDB-Version	Version der IKARUS Spam Datenbank
UDB-Version	Version der IKARUS URL Datenbank
Clusterstatus	Cluster Status
Ablaufdatum der Lizenz	Datum, wann die derzeit gültige Lizenz abläuft
User-Lizenzen	Wenn Ihre Lizenz auf eine bestimmte Useranzahl beschränkt ist, dann können Sie hier überprüfen, wie viele davon tatsächlich genutzt werden.
Aktualisieren-Button	Aktualisiert die gerade verwendeten User.

Tabelle 3: Serverinformationen



3.4 Globale Einstellungen

In dieser Einstellungsmaske werden die globalen Einstellungen von **IKARUS gateway.security** festgelegt.

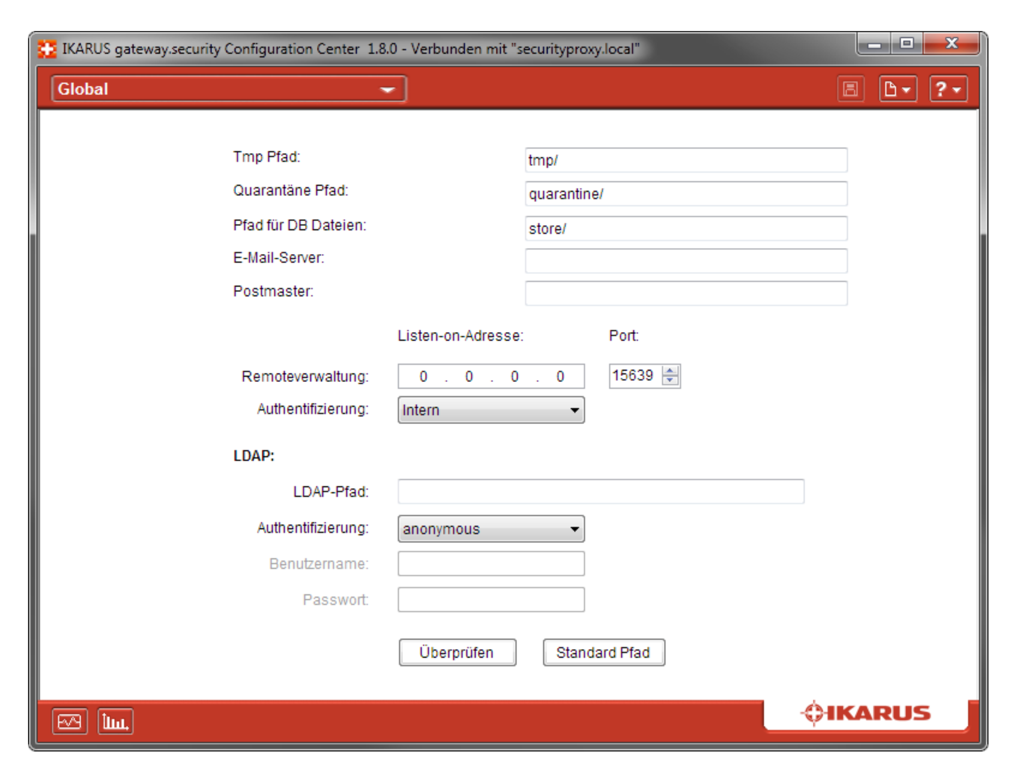


Abbildung 4: Globale Einstellungen



Wert	Beschreibung
Tmp Pfad	Der Pfad, unter welchem **IKARUS gateway.security** temporäre Dateien anlegt.
Quarantäne Pfad	Der Pfad, in welchem **IKARUS gateway.security** infizierte oder geblockte Dateien ablegt.
Pfad für DB-Dateien	Der Pfad, in welchem die Datenbankdateien für Reporting und Greylisting abgelegt werden.
E-Mail-Server	Der Mailserver (SMTP Server), welcher für das Versenden von Benachrichtigungen wie Informationen, Alerts etc. verwendet werden soll.
Postmaster	Jene E-Mail-Adresse, welche als Absender für das Versenden von automatisierten E-Mails verwendet wird.
Remoteverwaltung (Listen-on-Address, Port)	Die Adresse und der Port, auf welchem **IKARUS gateway.security** Verbindungen für die Verwaltung mit dem **IKARUS gateway.security Configuration Center** zulässt. Ist die eingetragene Adresse `0.0.0.0`, so ist eine Verbindung auf allen verfügbaren Netzwerkinterfaces möglich.
Authentifizierung	Die Art der Authentifizierung beim Remotemanager. Die Möglichkeiten sind hier: • Internal: mittels der proxyeigenen Benutzerverwaltung • LDAP: mittels des Active Directories

Tabelle 4: Globale Einstellungen

Wert	Beschreibung
LDAP-Pfad	Angabe des LDAP Pfades, siehe Bsp. eines LDAP Pfades.
Authentifizierung	Hier kann zwischen anonymer (anonymous) oder einfacher (simple) Authentifizierung ausgewählt werden. Bei „simple“ muss ein Benutzername und Passwort definiert werden.
Benutzername	Benutzer für die einfache Authentifizierung gegenüber eines LDAP Servers.
Passwort	Angabe des Passworts des Benutzers.
Button „Standard Pfad“	Wird das **IKARUS gateway.security Configuration Center** auf einem Rechner innerhalb einer Windows Domain ausgeführt, kann über diese Funktion der Standardpfad automatisiert eingetragen werden.
Button „Überprüfen“	Überprüft die obige Konfiguration. Zuvor ist ein Speichern der Konfiguration notwendig.

Tabelle 5: LDAP



Beispiel eines LDAP Pfades

```
ldap://dc.int.local/DC=int,DC=local?sAMAccountName,memberOf?sub?(objectClass=person)
```

`dc.int.local` ist der interne Domain Controller / LDAP server

Achtung: Bei einer normalen LDAP-Verbindung werden alle Daten im Klartext übertragen. Um eine sichere LDAP-Verbindung mit verschlüsselter Übertragung zu konfigurieren müssen Sie einfach nur ldap:// durch ldaps:// ersetzen und nach dem Server den Port :636 einfügen.

```
ldaps://dc.int.local:636/DC=int,DC=local?sAMAccountName,memberOf?sub?(objectClass=person)
```

3.5 Alarmierung

Hier können Sie Regeln festlegen, welche beim Eintreten bestimmter Ereignisse eine Alarmierung auslösen. Diese Alarmierungen können entweder in eine vordefinierte Logdatei geschrieben oder auch per E-Mail versandt werden.

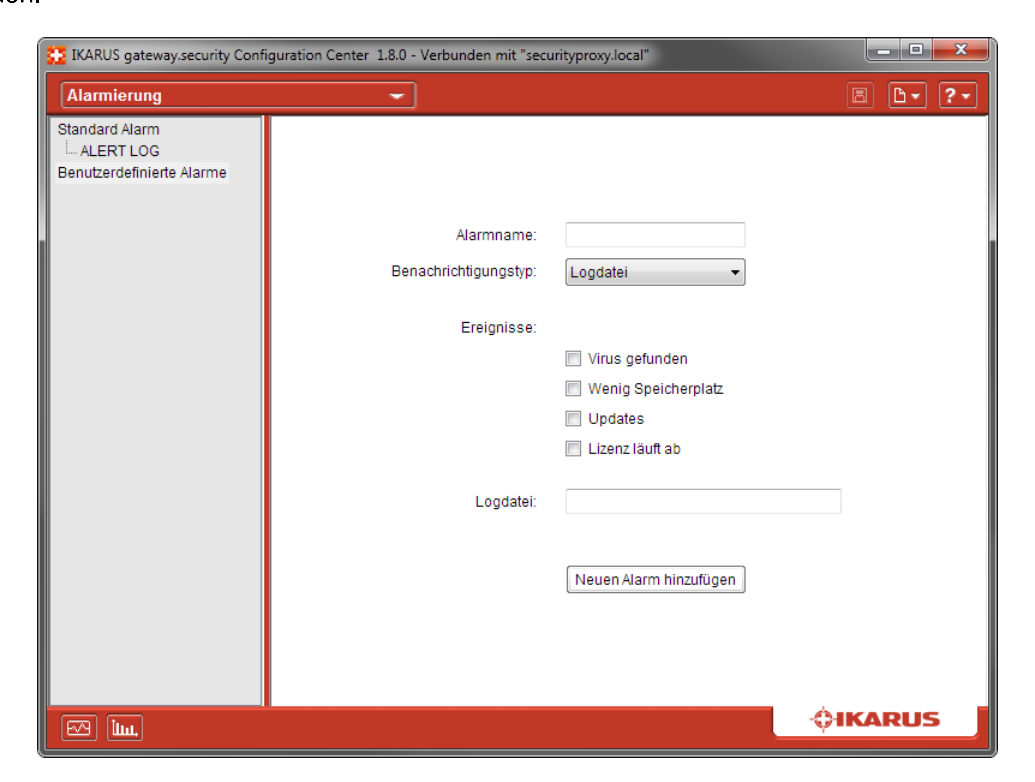


Abbildung 5: Alarmierung



Wert	Beschreibung
Alarmname	Der Name des Alarms
Benachrichtigungstyp	Auswahl ob Logdatei oder E-Mail
Ereignisse	Hier legen Sie fest, welche Ereignisse eintreten müssen, um einen Alarm auszulösen. Die möglichen Ereignisse sind • Virus gefunden • Wenig Speicherplatz • Updates • Lizenz läuft ab (jeweils 30 Tage, 14 Tage und unter 12 Tagen täglich vor Ablauf)
Logdatei/E-Mail	Abhängig vom Benachrichtigungstyp ist in dieses Feld entweder der Pfad der Logdatei oder die E-Mail-Adresse, an welche die Alarmierungen versandt werden sollen, einzutragen.
Button „Neuen Alarm hinzufügen“ / “Alarm löschen“	Beim Erfassen eines neuen Alarms wird dieser durch Betätigen des Buttons hinzugefügt. Desgleichen ist es möglich, bei bereits angelegten Alarmen diese über diesen Button zu löschen.

Tabelle 6: Alarmierung

3.6 Auto-Update

Hier ist es möglich, die Auto-Update-Funktionalität von **IKARUS gateway.security** festzulegen. Dadurch wird ermöglicht, dass **IKARUS gateway.security** immer auf dem aktuellsten Stand ist, um maximale Sicherheit zu gewährleisten. Bei aktiviertem Auto-Update versucht **IKARUS gateway.security** in regelmäßigen Abständen ein Auto-Update durchzuführen. Dies erfolgt in einem Intervall von 10 Minuten.

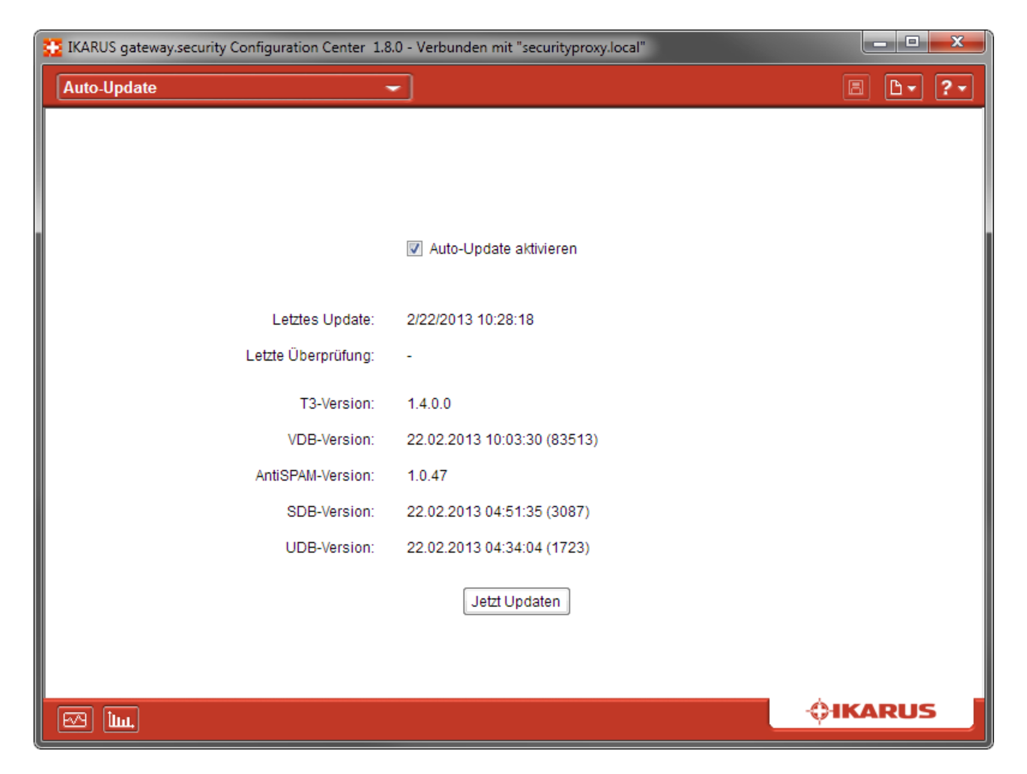


Abbildung 6: Auto-Update

Wert	Beschreibung
Auto-Update aktivieren	Bei aktivierter Checkbox ist die Auto-Update Funktion aktiv gesetzt.
Letztes Update	Gibt den Zeitpunkt an, zu welchem das letzte erfolgreiche Update durchgeführt wurde.
Letzte Überprüfung	Gibt den Zeitpunkt an, zu welchem zuletzt ein Auto-Update durchgeführt wurde (unabhängig davon ob dieses erfolgreich oder fehlgeschlagen war).
T3-Version	Version der IKARUS Scan Engine
VDB-Version	Version der IKARUS Virendatenbank
Antispam-Version	Version des IKARUS Antispam Plugins
SDB-Version	Version der IKARUS Spam Datenbank
UDB-Version	Version der IKARUS URL Datenbank
Button „Jetzt Updaten“	Manuelles Starten des Update Prozesses.

Tabelle 7: Auto-Update

3.7 Logging

Hier können Sie die Parameter für das Logging einstellen.

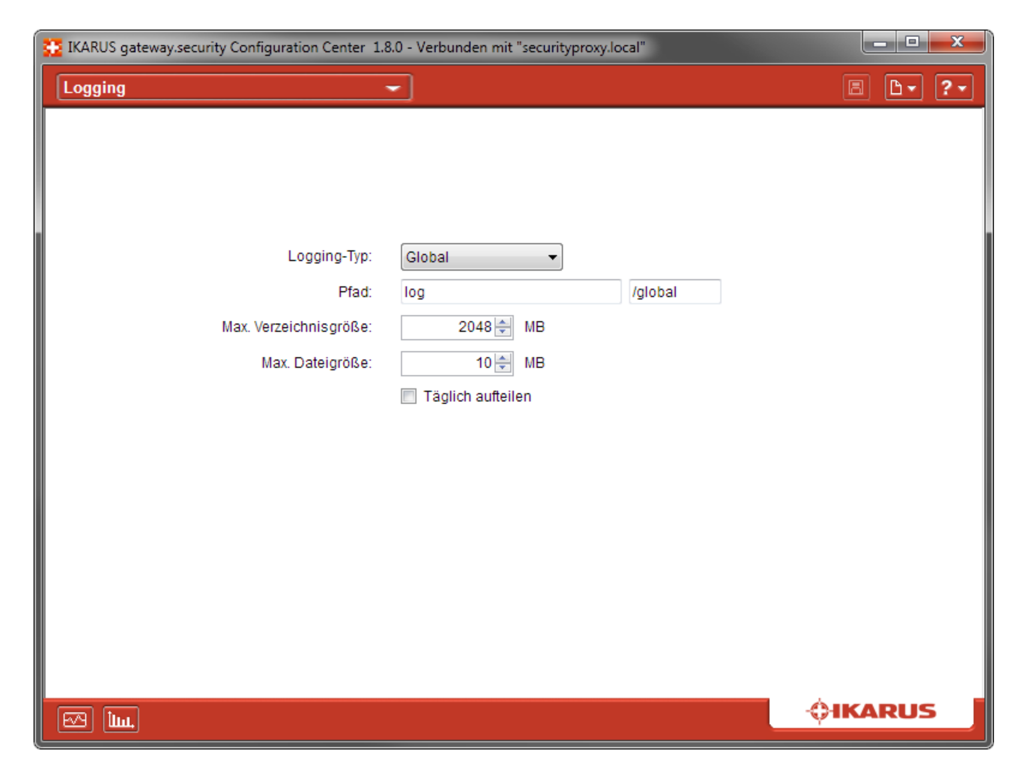


Abbildung 7: Logging

Wert	Beschreibung
Logging-Typ	Die Type des Logfiles, für welche die Einstellungen gelten. Es sind die folgenden vier Möglichkeiten auswählbar: • Global • Web • E-Mail • Debug
Pfad	Der Pfad, unter dem der ausgewählte Logging-Typ gespeichert werden soll. Standardmäßig ist diese Einstellung relativ zum Installationsverzeichnis von **IKARUS gateway.security**.
Max. Verzeichnisgröße	Die maximale Größe des Verzeichnisses, welches für Logfiles dieses Typs vorgesehen ist.
Max. Dateigröße	Die maximale Größe einer Logdatei.
Täglich aufteilen	Am Anfang eines Tages wird die alte Logdatei gespeichert und eine neue begonnen.

Tabelle 8: Logging



3.8 Userverwaltung

Über die Userverwaltung wird der administrative Zugriff auf **IKARUS gateway.security** definiert.

3.8.1 Globale User

User werden in einer Passwort-Datei gemeinsam mit ihren verschlüsselten Passwörtern gespeichert. Die Userverwaltung ist simpel. User anlegen bzw. löschen oder Passwörter setzen bzw. ändern können Sie hier.

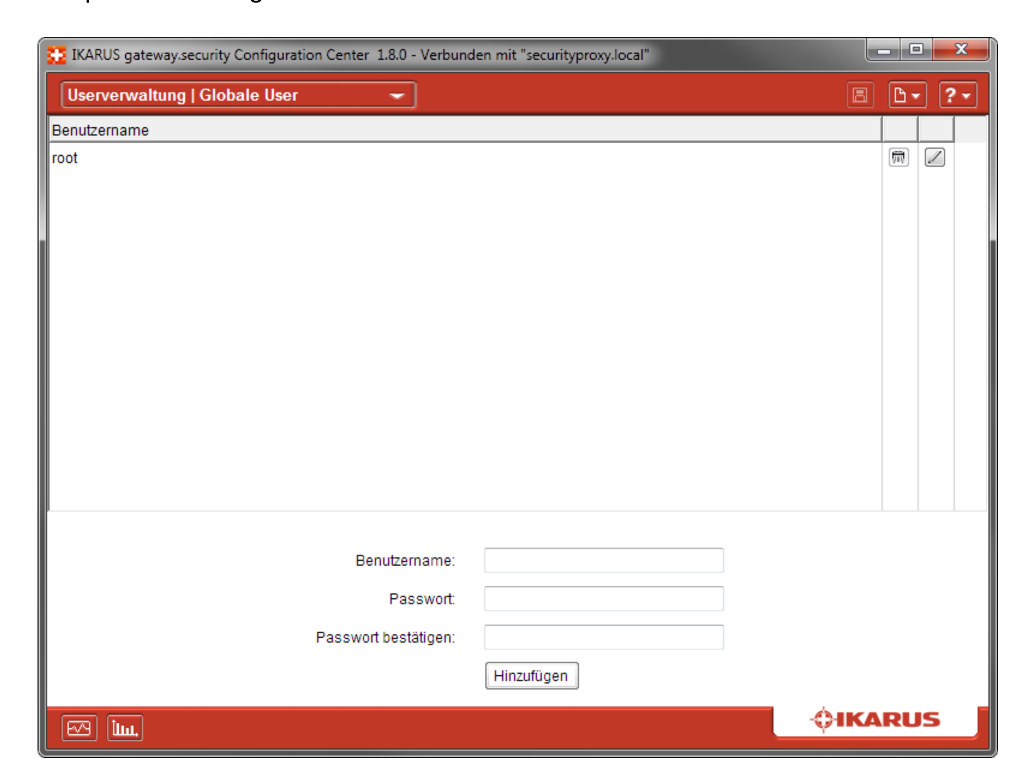


Abbildung 8: Globale User

3.8.2 Remotemanager

Der Zugriff kann aufgrund der Quell-IP-Adresse und der User-ID gesteuert werden.

Es gibt einen vordefinierten Admin-User mit der User-ID „ROOT“. Dieser User kann nicht entfernt werden. Nach einer Neu-Installation ist dessen Passwort neu zu setzen.

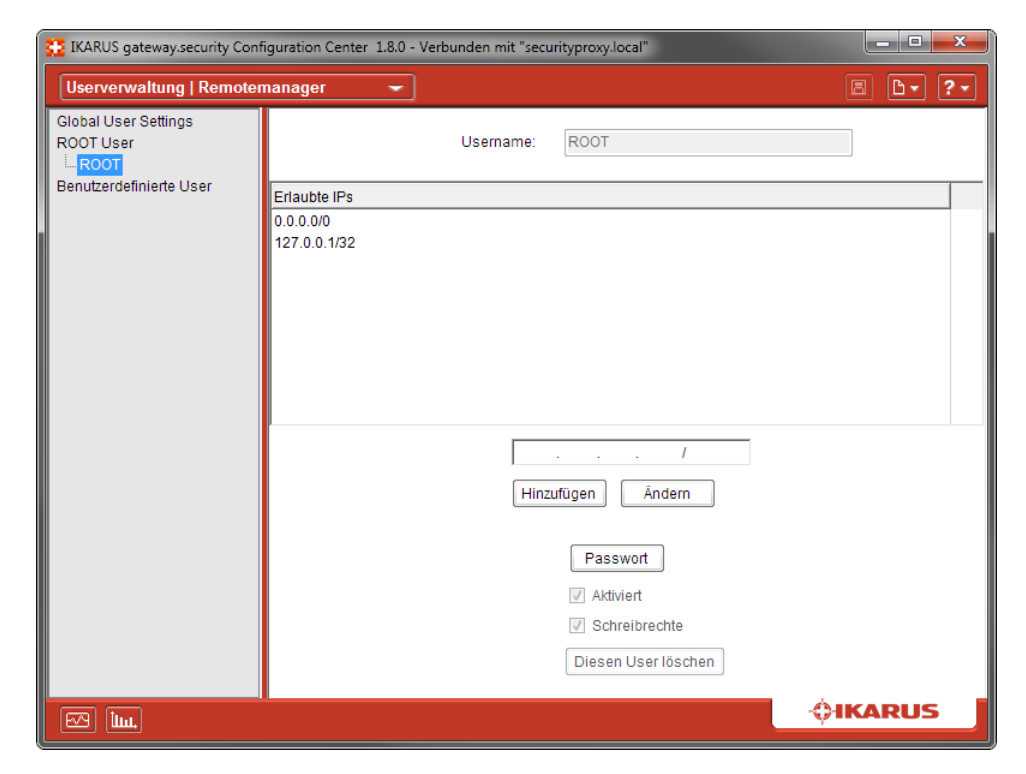


Abbildung 9: Remotemanager

Wert	Beschreibung
Global User Settings	Zugriffregelung basierend auf der Quell-IP-Adresse. Standard Einstellung: Jede IP-Adresse inkl. des „localhost“ hat Zugriff auf das Management von **IKARUS gateway.security**. Falls die Administration ausschließlich am Server direkt erfolgen soll (**IKARUS gateway.security Configuration Center** und das Backend **IKARUS gateway.security** sind am selben Server (Microsoft) installiert) kann der Zugriff auf den Eintrag „localhost“ eingeschränkt werden.
ROOT User	Kann nicht gelöscht werden. Einschränkung auf bestimmte Quell-IP-Adressen möglich. Passwort-Änderung möglich.
Benutzerdefinierte User	Unter Angabe eines Benutzernamens und Auswahl des „Hinzufügen“-Buttons wird ein neuer Benutzer hinzugefügt Auch hier kann auf Quell-IP-Adressen eingeschränkt werden Soll der neue Benutzer Schreibrechte erhalten, ist das Recht „Schreibrechte“ zu wählen. Ein Benutzer kann auch über den Button „Diesen User löschen“ entfernt werden.

Tabelle 9: Remotemanager Userverwaltung



3.9 Web-Einstellungen

IKARUS gateway.security erlaubt den Betrieb eines HTTP- sowie eines FTP-Proxys.

In den Proxy-Einstellungen eines Web-Clients kann auch ein Proxy für HTTPS definiert werden. Dies ist selbstverständlich auch mit **IKARUS gateway.security** möglich. Im Falle von HTTPS wird der verschlüsselte Datenverkehr zwischen Client und Ziel-HTTPS-Server durch getunnelt. Bitte beachten Sie, dass in diesem Fall kein AntiViren-Schutz am Gateway erfolgt. Ohne zusätzlichen Konfigurationsaufwand und ohne zusätzliche Software wäre dies auch nicht möglich. IKARUS Security Software bietet optional ein HTTPS-PlugIn in Form einer Zusatz Applikation an, die es Ihnen ermöglicht, https auf Malware zu überprüfen. Bitte wenden Sie sich an **IKARUS** falls Sie daran interessiert sind.

3.9.1 HTTP-Proxy

Über diese Eingabemaske können Sie die Einstellungen für den HTTP-Proxy definieren und verändern.

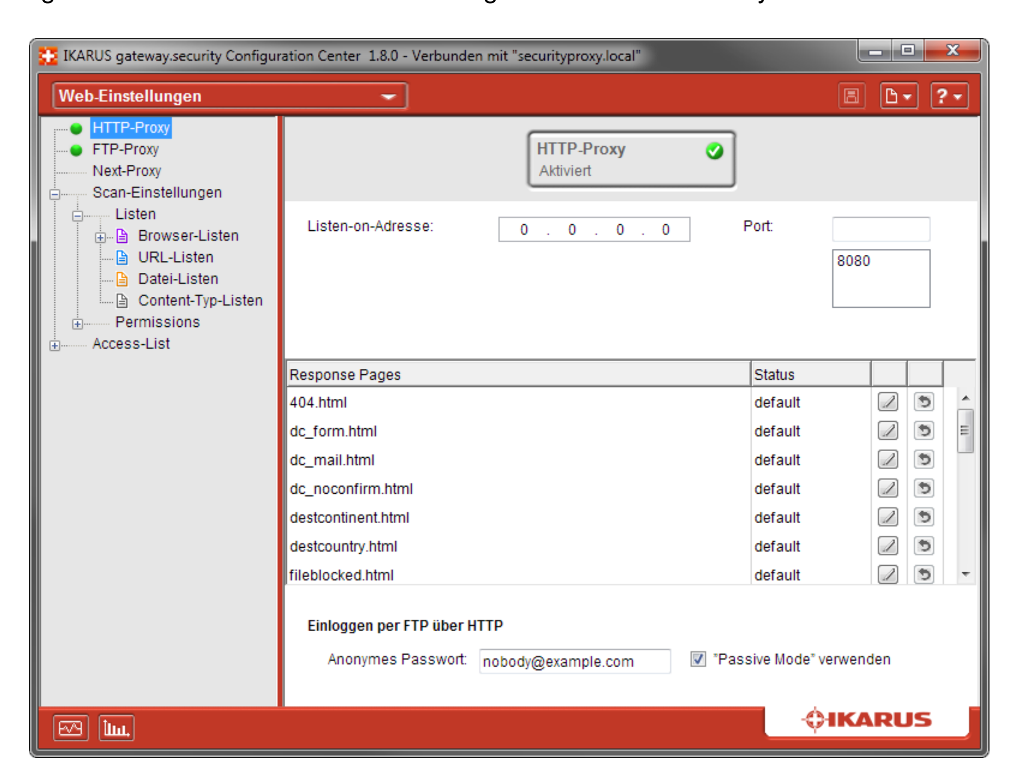


Abbildung 10: HTTP-Proxy

Wert	Beschreibung
Button „HTTP-Proxy“	Aktiviert bzw. deaktiviert den HTTP-Proxy. Achtung: Änderungen werden erst nach dem Speichern aktiv.
Listen-on-Adresse	Die IP Adresse, auf dieser **IKARUS gateway.security** den HTTP-Proxydienst anbietet. Auf Systemen mit mehreren Netzwerk-Interfaces ist es möglich, den Proxydienst auf allen verfügbaren Interfaces anzubieten. In diesem Fall geben Sie die IP-Adresse `0.0.0.0` ein.
Port	Der Port (oder wahlweise auch mehrere Ports), an welchem der HTTP-Proxydienst angeboten wird. Standardmäßig ist dies der Port 8080, aber Sie können hier jeden verfügbaren, nicht von einem andern Service verwendeten Port eintragen. Achtung: Sollten Sie einen Port wählen, der von einem anderen Service oder Programm verwendet wird, kann es zu Konflikten kommen.
Response Pages	Dies ist eine Liste der Response Pages, HTML-Seiten, welche an den Browser gesandt werden, falls z.B. eine Seite blockiert wird oder eine schadhafte Datei gefunden wurde. Über Auswahl des Editier-Symbols beim entsprechenden Listeneintrag können Sie sich den HTML-Code der jeweiligen Response-Page anzeigen lassen. Sie haben die Möglichkeit, die Response Pages zu verändern und Ihren Bedürfnissen anzupassen. Hierfür benötigen Sie allerdings HTML-Kenntnisse und im Bedarfsfall über entsprechende Grafiken. Sollten Sie daher keine gebrandeten Response Pages benötigen, empfehlen wir, die Default-Response Pages zu verwenden.
Anonymes Passwort	Jenes Passwort, welches bei FTP Verbindungen über HTTP verwendet wird.
Passive Mode verwenden	Wenn aktiviert, verwendet **IKARUS gateway.security** bei FTP über HTTP den passiven Modus.

Tabelle 10: HTTP-Proxy

3.9.2 FTP-Proxy

IKARUS gateway.security verfügt auch über einen eigenen Proxydienst für das FTP-Protokoll. Dieser bietet einen effektiven Schutz gegen schadhafte Software, die via FTP auf einen Computer gelangen kann.

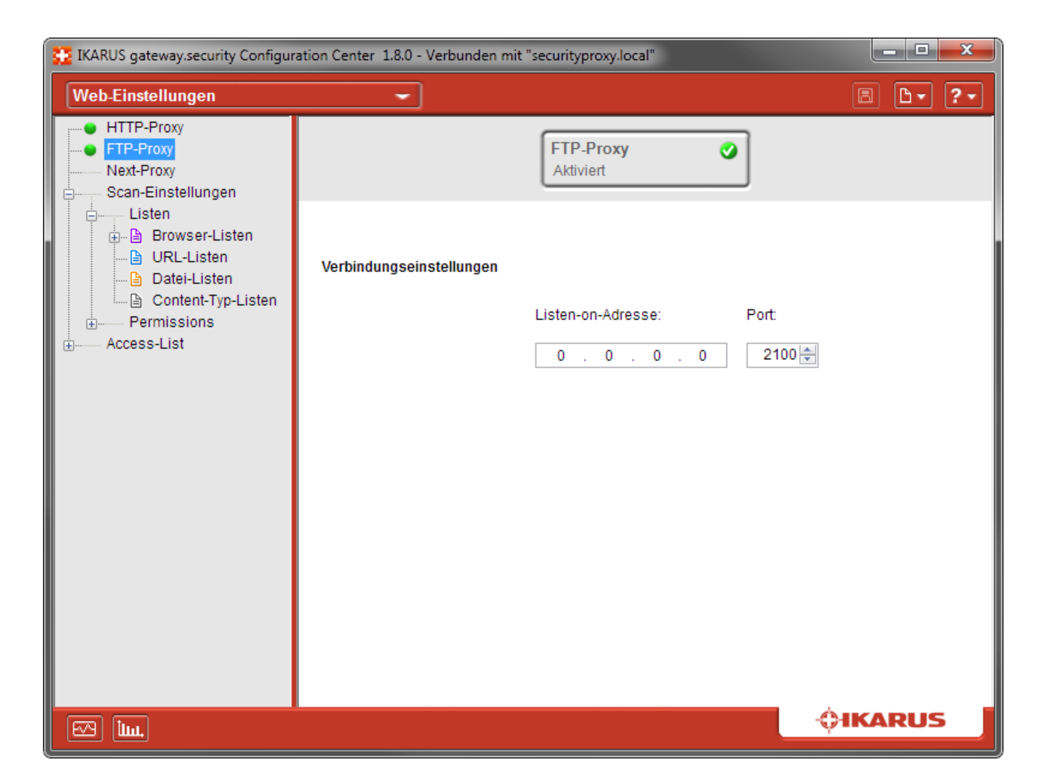


Abbildung 11: FTP-Proxy

Wert	**Beschreibung**
Button „FTP Proxy“	Mit diesem Button kann der FTP-Proxy aktiviert bzw. deaktiviert werden. Achtung: Änderungen werden erst nach dem Speichern aktiv.
Listen-On Adresse	Die IP Adresse, auf dieser **IKARUS gateway.security** den FTP-Proxydienst anbietet. Auf Systemen mit mehreren Netzwerk-Interfaces ist es möglich, den Proxydienst auf allen verfügbaren Interfaces anzubieten. In diesem Fall geben Sie die IP-Adresse 0.0.0.0 ein.
Port	Der Port, an welchem der FTP-Proxydienst angeboten wird. Standardmäßig ist dies der Port 2100, aber Sie können hier jeden verfügbaren, nicht von einem andern Service verwendeten Port eintragen. Achtung: Sollten Sie einen Port wählen, der von einem anderen Service oder Programm verwendet wird, kann es zu Konflikten kommen.

Tabelle 11: FTP-Proxy

3.9.3 Next Proxy

Es ist möglich, **IKARUS gateway.security** mit einem anderen Proxy-Server zusammenzuschalten. Für diesen Fall müssen dessen Verbindungsdaten erfasst werden, damit **IKARUS gateway.security** Anfragen an den



anderen Proxyserver weiterleiten kann.

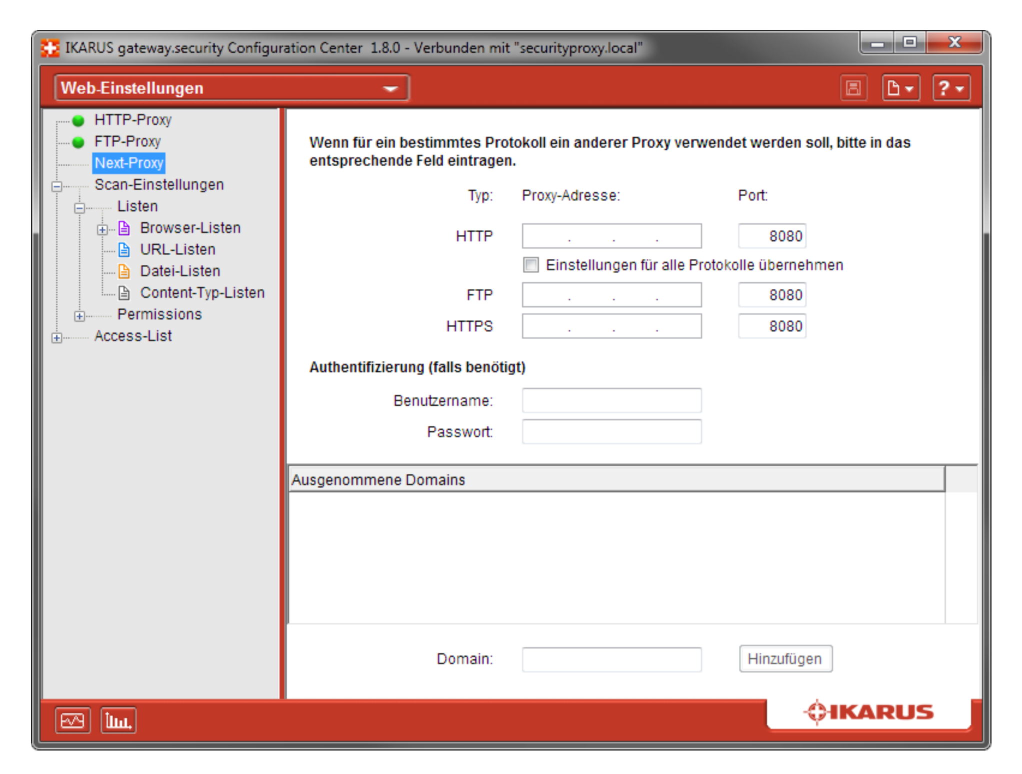


Abbildung 12: Next Proxy

Wert	Beschreibung
HTTP Proxy Adresse	Die IP-Adresse des Next-Proxy, an den HTTP-Anfragen weitergeleitet werden sollen.
HTTP Proxy Port	Der Port, an welchem der Next-Proxy den HTTP-Proxydienst anbietet.
Einstellungen für alle Protokolle übernehmen	Ist diese Checkbox aktiviert, werden die Einstellungen für den HTTP-Proxy auch für FTP und HTTPS übernommen.
FTP Proxy Adresse	Die IP-Adresse des Next-Proxy, an den FTP-Anfragen weitergeleitet werden sollen.
FTP Proxy Port	Der Port, an welchem der Next-Proxy den FTP-Proxydienst anbietet.
HTTPS Proxy Adresse	Die IP-Adresse des Next-Proxy, an den HTTPS-Anfragen weitergeleitet werden sollen.
HTTPS Proxy Port	Der Port, an welchem der Next-Proxy den HTTPS-Proxydienst anbietet.
Benutzername und Passwort	Falls der Next-Proxy eine Authentifizierung verlangt, so können Sie in diesen beiden Feldern den benötigten Benutzernamen und das dazugehörige Passwort erfassen.
Ausgenommene Domains	Dies ist eine Liste jener Domains, welche vom Routing auf den Next-Proxy ausgenommen sind. Sie können neue Domainserfassen, indem Sie diese im Feld Domain eintragen und mittels eines Klicks auf das Feld „Hinzufügen“ der Liste hinzufügen.

Tabelle 12: Next Proxy - Proxychain

3.9.4 Scan-Einstellungen

Über die Scan-Einstellungen können Sie Regeln für den HTTP-Proxy definieren. Diese Möglichkeiten, die Ihnen **IKARUS gateway.security** hier bietet, sind sehr umfangreich und mächtig.

Listen

- Browser-Listen
- URL-Listen
- Datei-Listen
- Content-Type-Listen

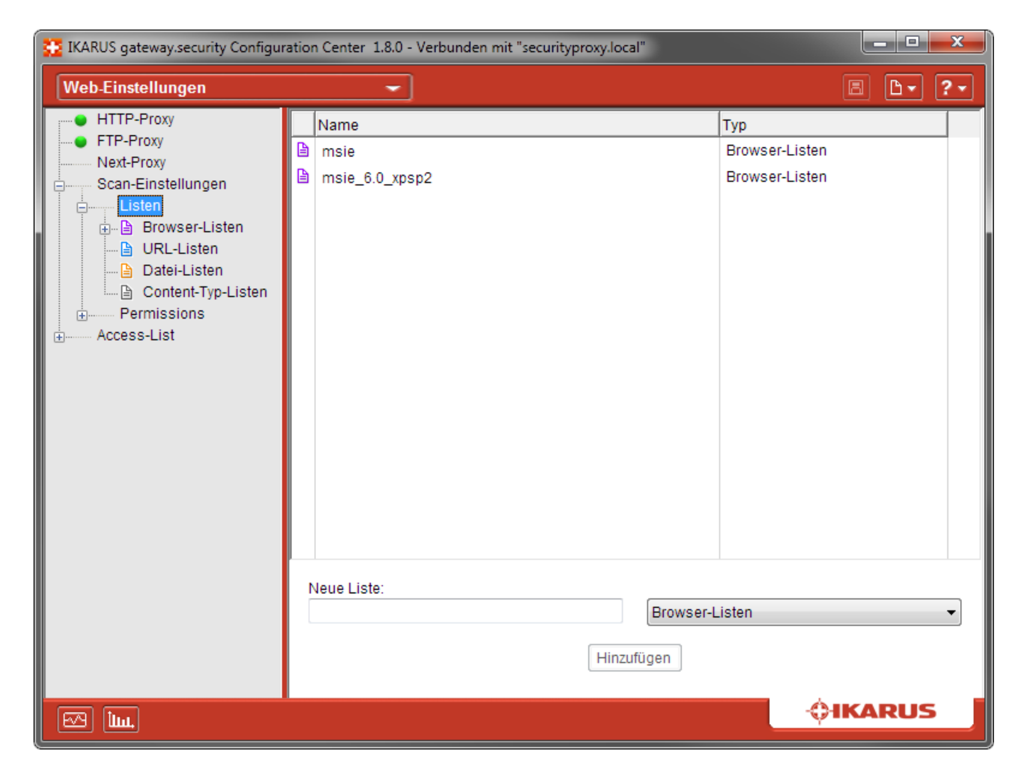


Abbildung 13: Listen

Wert	Beschreibung
Übersicht	Gibt Name und Typ der erfassten Liste an.
Neue Liste	Tragen Sie hier den Namen jener Liste ein, die Sie neu anlegen wollen.
Listen-Typ	Aus dieser Listbox können Sie auswählen, welcher Art (Browser-Liste, URL-Liste, Datei-Liste, MIME-Type-Liste) die neue Liste ist.
Button „Hinzufügen“	Fügt den neuen Eintrag der Übersicht hinzu. Desgleichen erscheint die neugeschaffene Liste an der richtigen Stelle im Baum im linken Fensterbereich.

Tabelle 13: Listen

Jeder neugeschaffenen Liste können Sie wiederum neue Einträge hinzufügen. Hierzu wählen Sie im Baum im linken Fensterbereich die richtige Listen-Kategorie aus.

Browser-Listen

Hier können Sie Listen von Webbrowsern erstellen. **IKARUS gateway.security** ist in der Lage, auf Basis des Browsers zu filtern. Somit ist es beispielsweise möglich, den Internetzugang für bestimmte Webbrowser frei zu geben oder zu sperren. Dies ist dann notwendig, wenn z.B. die Unternehmensrichtlinie die Verwendung eines bestimmten Browsers vorschreibt.

Basierend auf dem User Agent String, den jeder Browser bei der Übermittlung von Daten via HTTP an den Server sendet, ist es **IKARUS gateway.security** möglich, eine browserbasierte Filterung der Daten zu ermöglichen.



Der Internet Explorer 8.0 meldet sich beispielsweise mit dem User Agent String `Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64)` während sich Mozilla Firefox auf Windows mit `Mozilla/5.0 (Windows; U; Windows NT 6.1; en-GB; rv:1.9.2.13) Gecko/20101203 Firefox/3.6.13.` identifiziert.

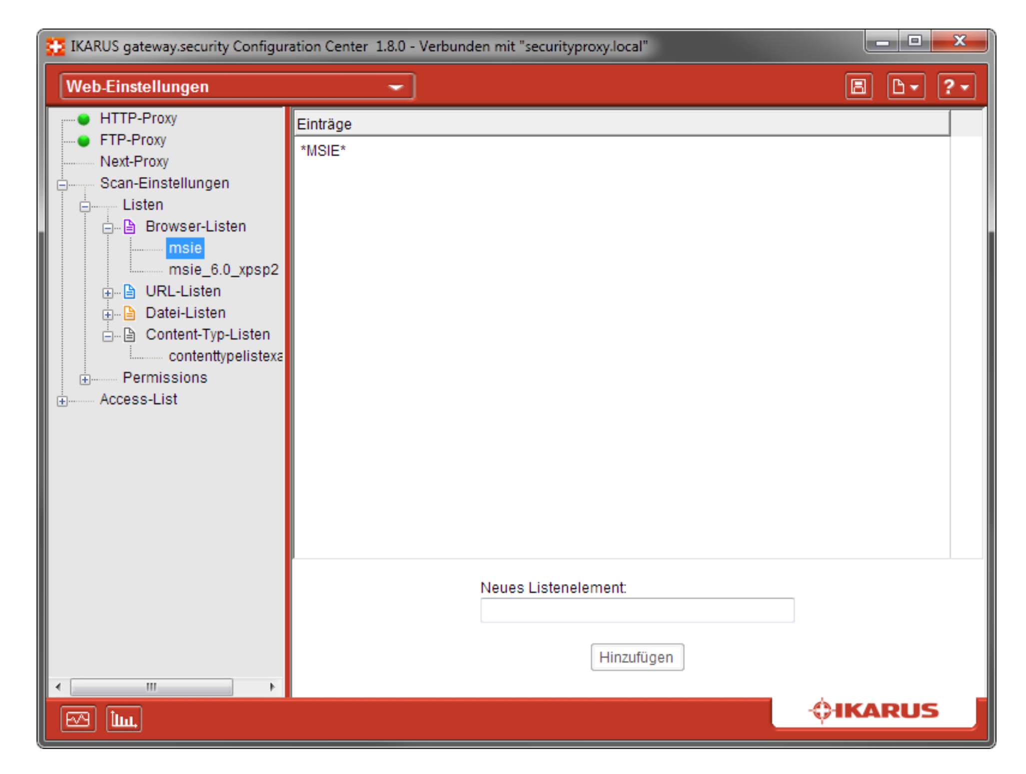


Abbildung 14: Beispielliste

Anhand der User Agent Strings können Sie Browserlisten zusammenstellen. Bei der String-Erstellung können Sie auch Wildcards benutzen. Als Wildcard wird das Zeichen * benutzt. Sie können z.B. mit dem String *msie* sämtliche Versionen des Internet Explorers zusammenfassen.

Falls Sie nicht wissen, wie Sie den User Agent String Ihres Browsers in Erfahrung bringen, rufen Sie einfach folgende Webseite auf: http://www.useragentstring.com. Alternativ können Sie aber auch die Client/Server-Kommunikation mit Hilfe eines Network Sniffers wie z.B. Wireshark herausfinden.

URL-Listen

In den URL-Listen können Sie URLs zusammenfassen, die Sie dann später bei der Anlage von Regeln verwenden können, um den Zugriff auf diese zu erlauben oder zu verbieten. Eingegeben werden können URLs hier nur in ASCII-Zeichen (ohne Blank).

Datei-Listen

In den Dateilisten können Sie bestimmte Dateinamen definieren, die in weiterer Folge bei der Regelanlage verwendet werden können, um den Zugriff auf diese zu erlauben oder zu verbieten.

Es ist möglich, entweder komplette Dateinamen zu erfassen (z.B. meineDatei.doc) oder durch den Einsatz von Wildcards beispielsweise alle Dateien, die eine bestimmte Datei-Endung besitzen (z.B. *.gif).



Content-Type Listen

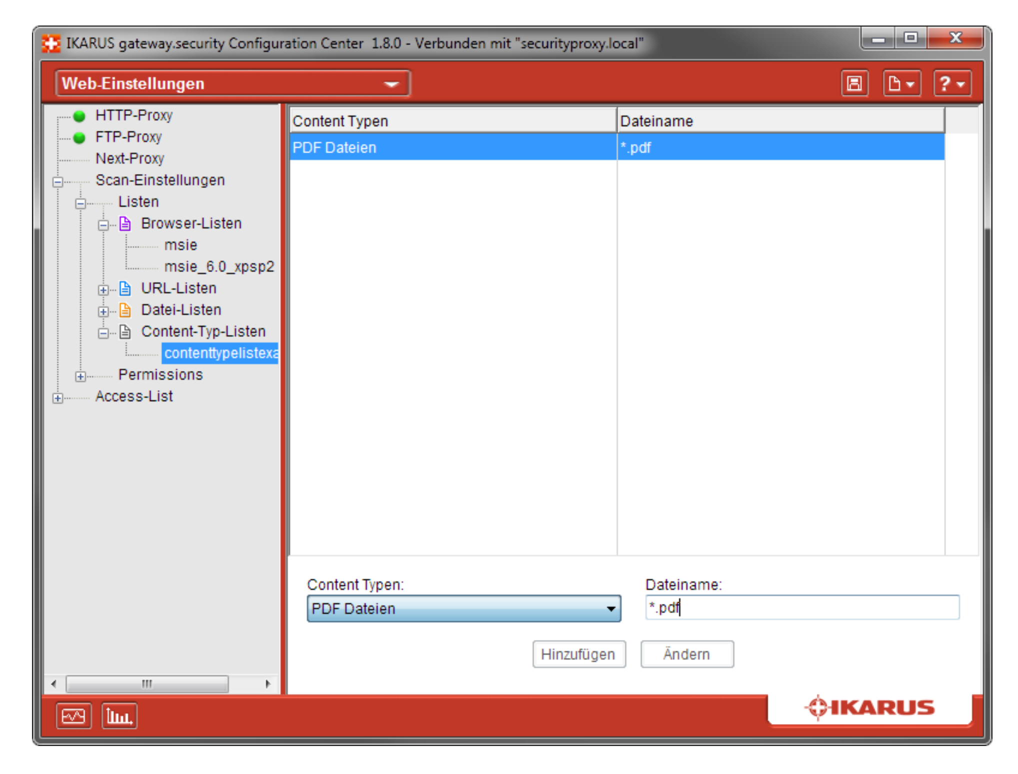


Abbildung 15: Beispiel Content-Type Liste

In dieser Ansicht können Sie Content-Type Listen erfassen. Im Gegensatz zu den Datei-Listen sind Content-Type Listen ein viel mächtigeres Instrument, um Dateigruppen zu filtern. Anders als bei den Datei-Listen wird hier nicht nach Datei-Endung gefiltert, sondern nach der tatsächlichen Dateiart. Dies ist insofern ein effektives Mittel, da eine Datei-Endung nichts über die tatsächliche Beschaffenheit einer Datei aussagt (so kann z.B. eine ausführbare Datei mit der Datei-Endung .jpg ausgestattet werden, obwohl es keine Grafik ist). Somit könnte unter Umständen Malware auf Ihren Rechner gelangen.

Content-Types schaffen hierbei Abhilfe, da sie die Dateien nach ihrem Typ filtern und so erkennen, um welche Art von Datei es sich handelt.

Die derzeit von **IKARUS gateway.security** unterstützten Content-Types sind:

Content Type	German Name	English Name
Any	Alle Dateien	All Files
Archive	Archivdateien	Archive Files
Executables	Ausführbare Dateien	Executable Files
MS Office	Office-Dateien	Office Files
Adobe Acrobat Document	PDF-Dateien	PDF Files
Audio	Audio-Dateien	Audio Files
Video	Video-Dateien	Video Files
MS Word	Word-Dateien	Word Files
MS Excel	Excel-Dateien	Excel Files
MS PowerPoint	PowerPoint-Dateien	PowerPoint Files
MS Visio	Visio-Dateien	Visio Files

Tabelle 14: Content-Type Informationen

Sie können diese Content-Types aus dem hierfür Drop-down-Feld Content-Type auswählen. Zusätzlich können Sie noch einen Dateinamen erfassen, der den Filter weiter einschränkt. Hierbei ist auch der Einsatz einer Wildcard (*) möglich. Lassen Sie das Feld Dateiname leer, so sind alle Dateien vom ausgewählten Content-Type betroffen.

Permissions

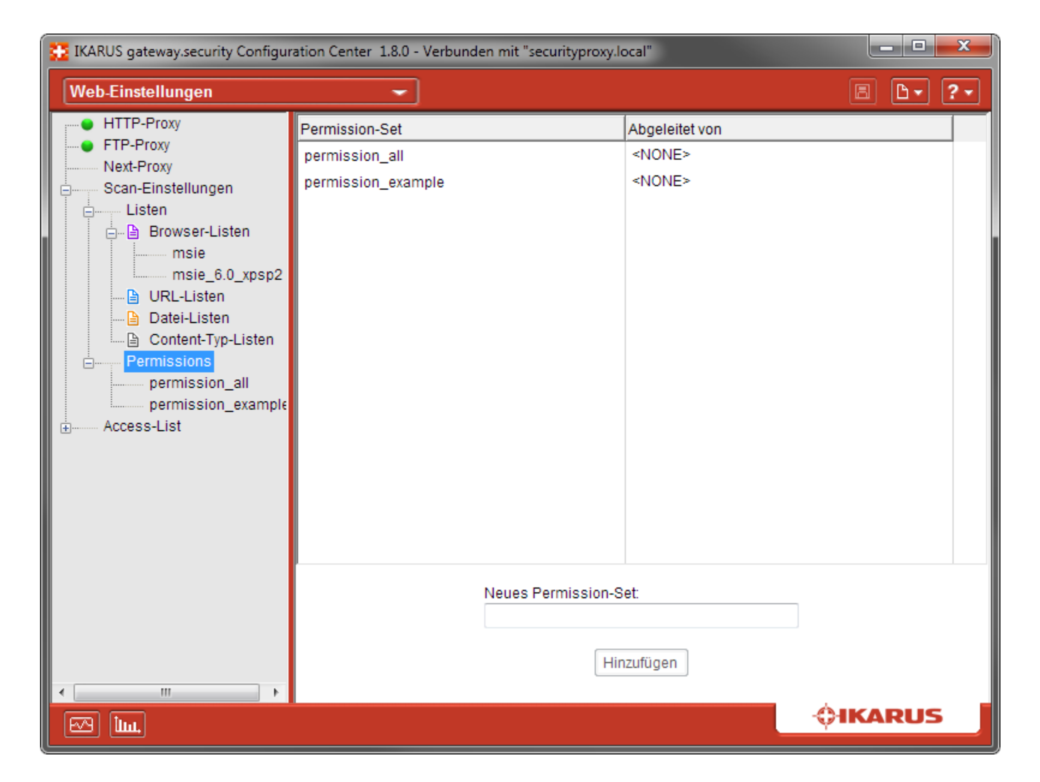


Abbildung 16: Permissions

In den Permissions werden die in den Listen zusammengefassten Filter zu Permission-Sets zusammengefasst. Hier können Sie die verschiedenen, vorher erfassten Listen eintragen, diese erlauben oder verbieten und in



verschiedener Form kombinieren.

Ein Permission-Set besteht aus einer Liste von Regeln, die entsprechend ihrer Priorität abgearbeitet werden. Das Ergebnis der ersten zutreffenden Regel wird angewandt, d.h. der Zugriff entweder erlaubt oder verboten.

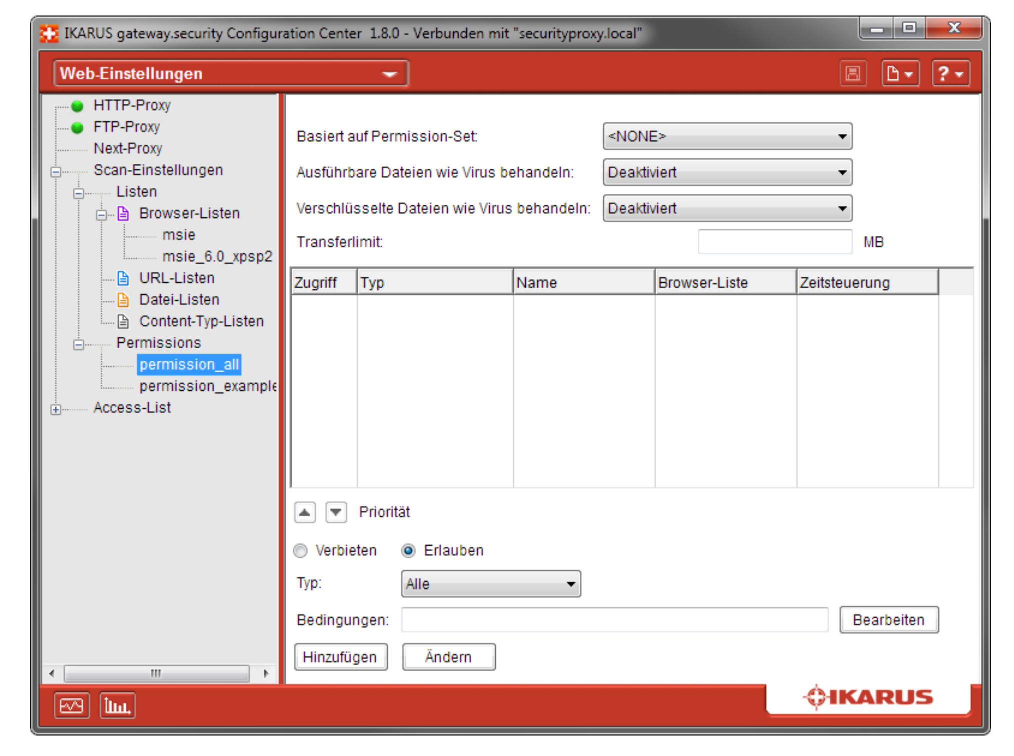


Abbildung 17: Permission-Sets

Wert	Beschreibung
Basiert auf Permission-Set	Hier können Sie auf ein anderes, bereits angelegtes Permission-Set verweisen. Die dort angelegten Rechte werden von diesem Permission-Set geerbt.
Ausführbare Datei wie Virus behandeln	Wenn aktiviert, werden ausführbare Dateien (Executables) behandelt, als wären sie schadhafte Software und gelöscht. Falls das Permission-Set von einem anderen Permission-Set abgeleitet wird, können die Einstellungen hier mit der Option „Erbt“ übernommen werden.
Verschlüsselte Dateien wie Virus behandelt	Wenn aktiviert, werden verschlüsselte Dateien wie Viren behandelt und gelöscht. Falls das Permission-Set von einem anderen Permission-Set abgeleitet wird, können die Einstellungen hier mit der Option „Erbt“ übernommen werden.
Transferlimit	Legt die maximale Datenmenge fest, die übertragen werden darf.
Übersichtsliste	In dieser Übersichtsliste werden alle diesem Permission-Set zugeordneten Regeln angezeigt.
Priorität	Erhöht oder verringert die Priorität der markierten Regel.
Erlauben/Verbieten	Das Ergebnis der Regel.
Typ	In diesem Drop-down Feld kann ein Kriterium für die Regel ausgewählt werden. Abhängig vom gewählten Eintrag werden Felder zur Erfassung des Wertes für dieses Kriterium eingeblendet. Zur Auswahl stehen • Alle • URL-Listen • URL • Content-Type-Listen • Content-Type • Datei-Listen • Datei/Extension • URL-Filter-Kategorie
Bedingungen	Hier können Sie in einem Dialog weitere Kriterien für die Regel definieren, wobei die Regel nur zur Geltung kommt, wenn alle Bedingungen zutreffen. Zur Auswahl stehen **Browser-Liste**, **Zeitsteuerung über Wochentage** und **Zeitsteuerung über Uhrzeiten**.
Button „Hinzufügen“	Fügt die angelegte Regel dem Permission-Set hinzu.
Button „Ändern“	Ändert die markierte Regel.

Tabelle 15: Permissions

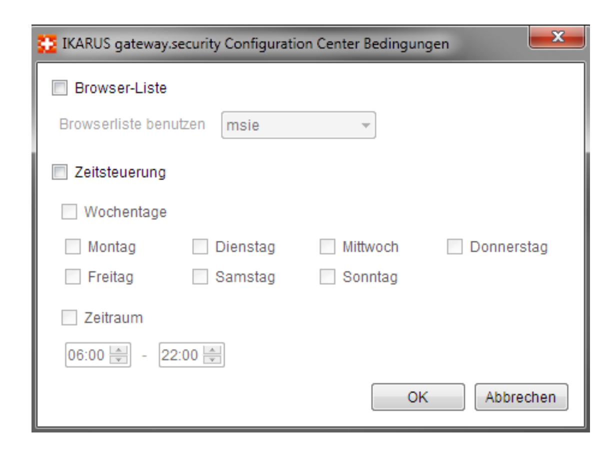


Abbildung 18: Bedingungen für Permission-Sets

URL-Filter-Kategorien

Der URL-Filter ist ein weiteres, mächtiges Instrument von **IKARUS gateway.security**. Der URL-Filter umfasst eine fix vordefinierte Klassifizierung von URLs nach bestimmten Themengebieten (z.B. adult, ecommerce, malware, games etc.). Jeder dieser Kategorien sind URLs zugeordnet. Durch Auswählen und Hinzufügen dieser Kategorien zu einem Permission-Set können Sie sämtliche URLs in einer Kategorie erlauben oder verbieten. Der Inhalt dieser Listen wird von IKARUS Security Software regelmäßig upgedatet. Daher bietet die Anwendung von URL-Filtern einen bequemen und sehr sicheren Weg, unerwünschte Webseiten zu verbieten.

3.9.5 Access-List

In den Access-Lists können Sie die erfassten Permission-Sets auf IP-Adressen bzw. Subnetz-Basis zuordnen und aktivieren. Darüber hinaus können Sie die Authentifizierungsmethode festlegen, welche angewendet werden soll.

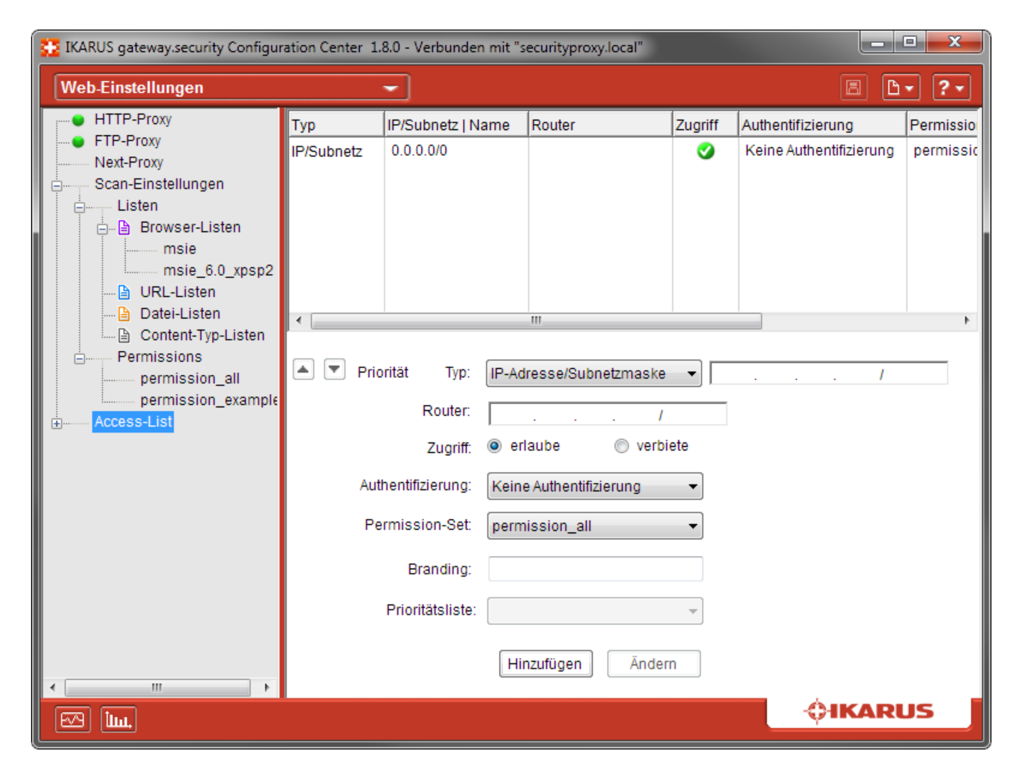


Abbildung 19: Access-List

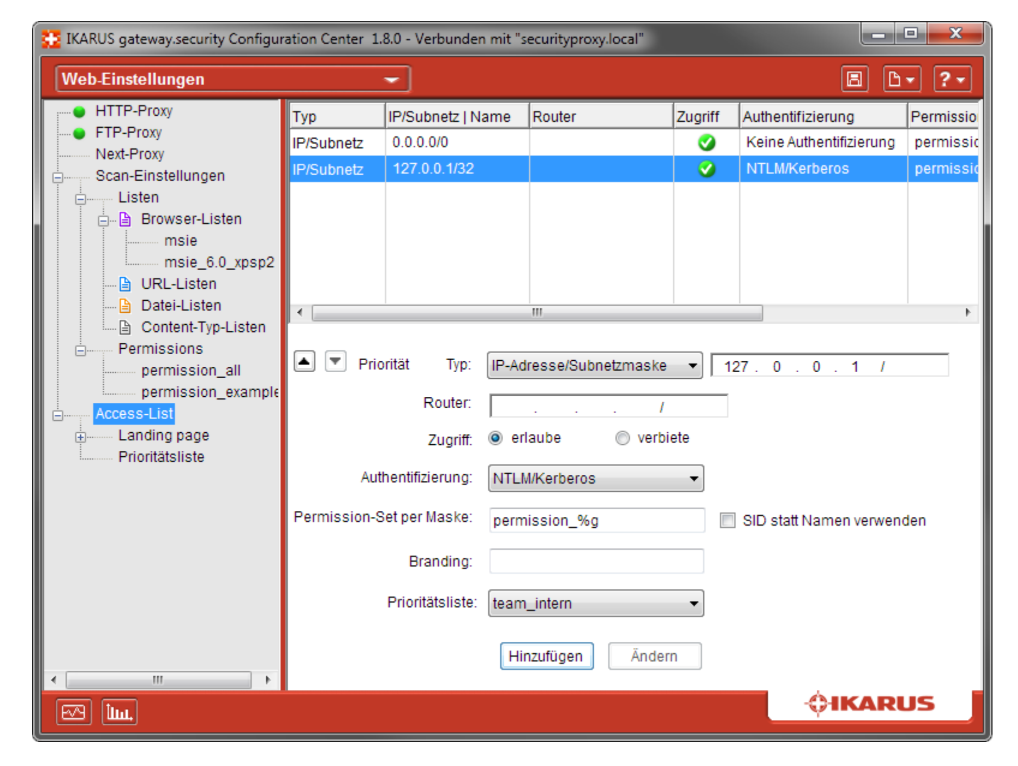


Abbildung 20: NTLM/Kerberos

Wert	Beschreibung
Übersichtsliste	In der Übersichtsliste werden die einzelnen IP-Addressen bzw. Subnetze angeführt, welche Art des Zugriffs (erlauben/verbieten) auf diese angewandt wird, welche Authentifizierungsmethode verwendet wird und das angewandte Permission-Set angezeigt.
Router	Definiert die IP-Adresse eines GRE-Routers, der für die IP-Adresse/das Subnetz verwendet wird.
Priorität	Hier können Sie die Priorität eines (vorher markierten) Eintrages in der Übersichtsliste erhöhen oder verringern.
Typ	Erlaubt die Erfassung einer IP-Adresse bzw. eines Netzwerkes.
Zugriff	Einen Eintrag erlauben oder verbieten.
Authentifizierung	Die Art der Authentifizierung, die auf das ausgewählte Netzwerk/IP-Adresse angewandt werden soll. Die Auswahlmöglichkeiten sind: • Keine Authentifizierung • Proxy-internal Authentifizierung • ISA-Firewall-Policy • LDAP Authentifizierung • NTLM/Kerberos (funktioniert nur unter Windows)
Permission-Set	Wählt das Permission-Set aus, das für diese Access-List verwendet werden soll.
Permission-Set per Maske	Wählt per Maske aus, welche Permission-Sets für diese Access-List in Frage kommen, mögliche Platzhalter sind %u und %g und erforderlich ist mindestens einer. Für weitere Informationen siehe 4.8.8.
SID statt Namen verwenden	Legt fest, dass bei der Ersetzung des Platzhalters in der Maske SIDs statt Namen für User und Gruppen genommen werden sollen.
Branding	Legt fest, welches *branding* für für dieses Netzwerk verwendet werden soll (siehe 4.4.2).
Prioritätsliste	Legt die Liste fest, die bestimmt, in welcher Reihenfolge Permission-Sets ausgewählt werden sollen, wenn mehrere Gruppen übereinstimmen.
Button „Hinzufügen“	Fügt den angelegten Datensatz der Übersichtsliste hinzu.
Button „Ändern“	Ändert einen (markierten) Datensatz in der Übersichtsliste.

Tabelle 16: Access-List

Prioritätslisten



In diesem Dialogfeld können Listen hinzugefügt und gelöscht werden, sowie Einträge zu den einzelnen Listen bearbeitet werden. Je nachdem, ob SIDs oder Namen verwendet werden, müssen entsprechende Einträge erstellt werden. Diese Listen dienen dazu, bei mehreren Gruppenübereinstimmungen eines Users zu ermitteln, für welche Gruppen zuerst nach einem gültigen Permission-Set gesucht werden soll. Hierfür kann mit den Pfeilen die Priorität der einzelnen Einträge festgelegt werden.

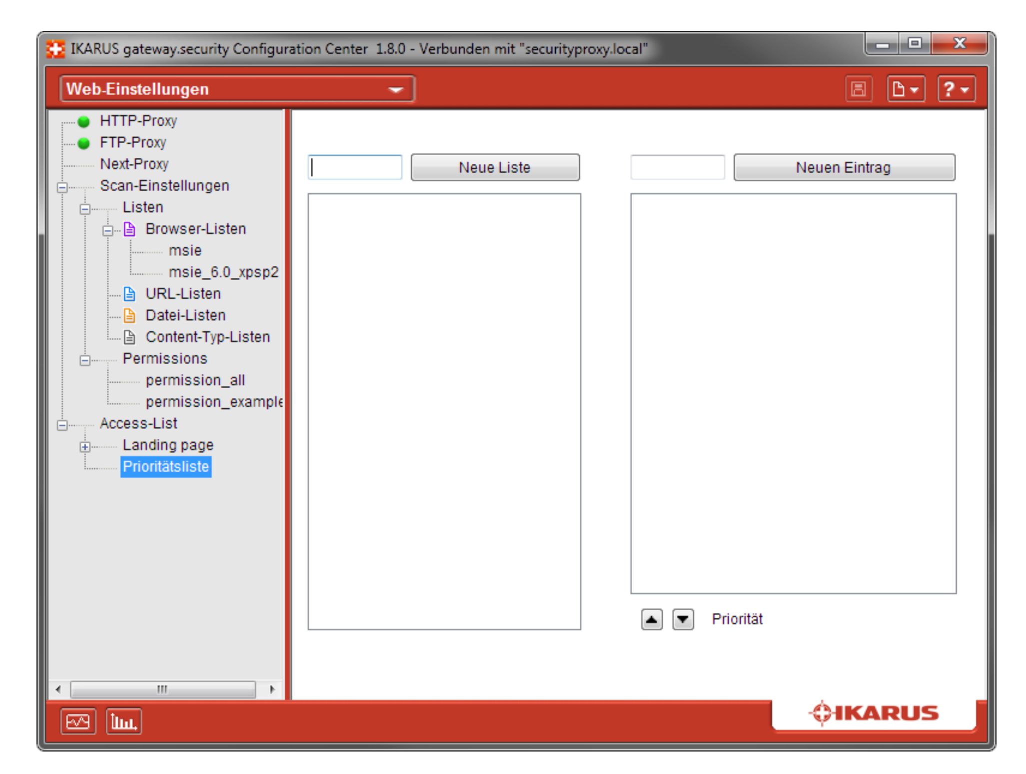


Abbildung 21: Prioritätslisten

3.10 E-Mail-Einstellungen

In den E-Mail Einstellungen sind alle scan-baren Protokolle zusammengefasst. Die Scan-Regeln können für die jeweiligen Protokolle zum Einsatz gebracht werden.



3.10.1 Scan-Regeln

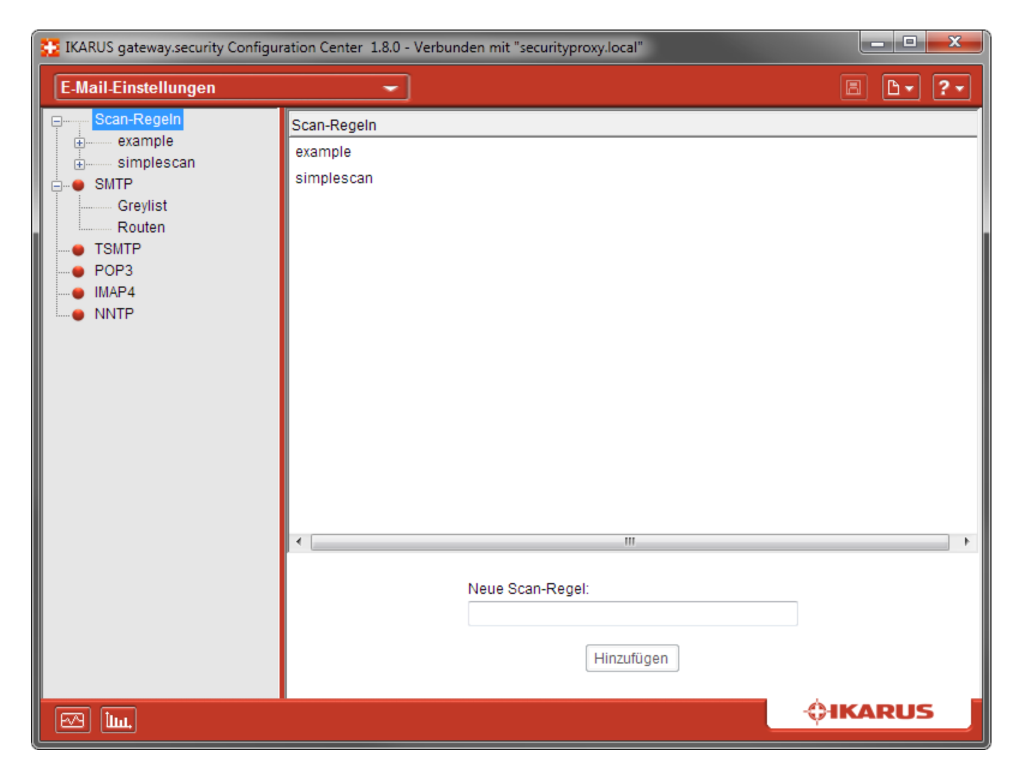


Abbildung 22: E-Mail-Einstellungen

Um einen effektiven Schutz zu gewährleisten ermöglicht **IKARUS gateway.security** eigene Scan-Regeln zu definieren. Es ist somit möglich, eigene Regeln für SPAM, E-Mail-Attachments und Malware festzulegen. Diese selbst definierten Regeln können für die folgenden Protokolle angewandt werden:

- SMTP
- TSMTP
- POP3
- IMAP4
- NNTP

Die maximale Anzahl von Regel-Sets ist nicht begrenzt. Sie können also verschiedene Regelsets für die diversen Protokolle angelegen. Bei SMTP ist es zusätzlich sogar möglich, Regeln auf Routen anzuwenden.

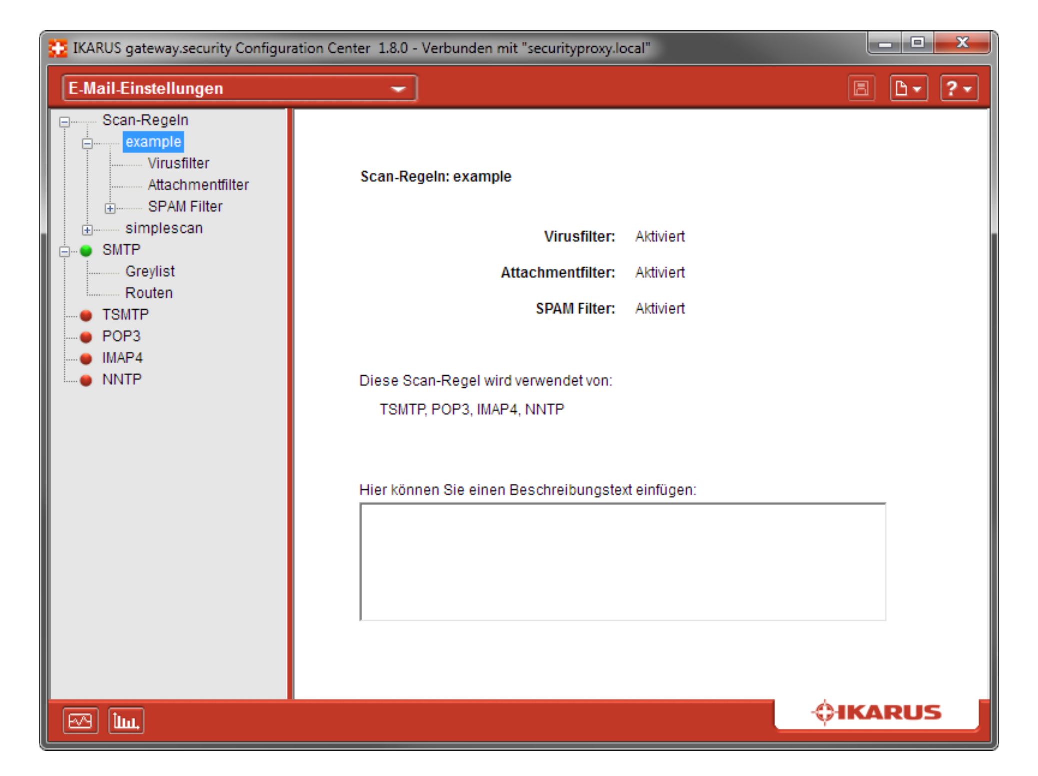


Abbildung 23: Scan-Regeln

Anlegen von Regeln

Der erste Schritt bei der Definition von Regeln ist die Anlage derselben. Sie können dabei den Namen selbst definieren, wobei zu beachten ist, dass der Name neben alphanumerischen nur die Zeichen -,_ und . enthalten darf. Sobald eine Scan-Regel hinzugefügt wurde, erscheint diese links in der Tree-View. Um die eben angelegte Regel zu bearbeiten, klicken Sie auf diese im Tree-View. Hier können Sie auf mehreren Ebenen Einstellungen vornehmen:

- Virusfilter
- Attachmentfilter
- SPAM Filter
- SPAM-Regeln

Virenfilter

Die Einstellungen für den Virenscanner sind die oberste Ebene der Scan-Regeln. Hier können Sie den Schutz durch den Virenscanner aktivieren und deaktivieren sowie dessen Verhaltensweise konfigurieren.

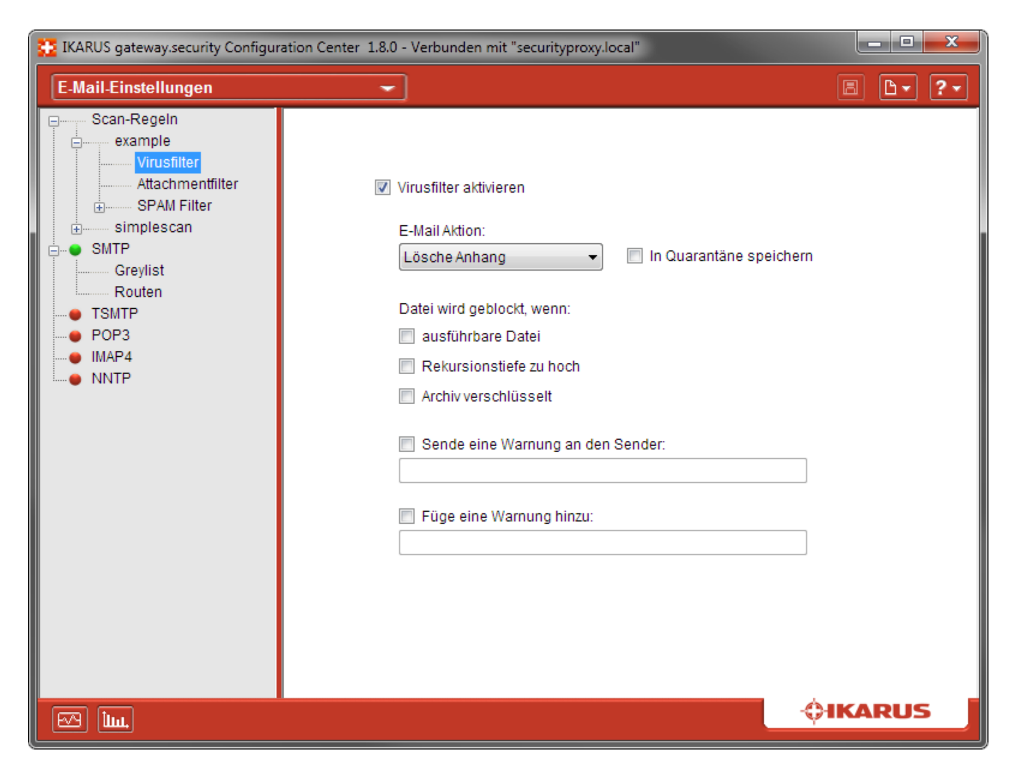


Abbildung 24: Virenfilter

Wert	Beschreibung
Virusfilter aktivieren	Diese Checkbox bestimmt, ob der Virenfilter aktiviert oder deaktiviert ist.
E-Mail Aktion	Bestimmt, welche Aktion durchgeführt werden soll, wenn ein Virus gefunden wurde. Die möglichen Aktionen sind "Lösche Anhang" und "Lösche E-Mail". Im ersten Fall wird nur der Anhang aus einer E-Mail entfernt, im letzteren Fall wird die gesamte E-Mail gelöscht.
In Quarantäne speichern	Ist diese Option aktiviert, werden die geblockten Dateien im Quarantäneverzeichnis des Servers gespeichert.
Datei wird geblockt wenn	
ausführbare Datei	Wenn es sich bei der betreffenden Datei um eine ausführbare Datei handelt, wird diese geblockt
Rekursionstiefe zu hoch	Wenn das rekursive Entpacken von Dateien eine gewisse Tiefe erreicht, werden diese geblockt (also wie ein Virus behandelt).
Archiv verschlüsselt	Wenn ein zu scannendes Archiv verschlüsselt ist, wird dieses geblockt.
Sende eine Warnung an den Sender	Ist diese Option aktiviert, so wird an den Absender eine Verständigung (Inhalt der Inputbox) versandt.
Füge eine Warnung hinzu	Fügt der E-Mail im Falle eines Virenfundes eine Warnung hinzu. Diese kann um einen Freitext (Inputbox) ergänzt werden.

Tabelle 17: Virenscanner



Attachmentfilter

Über den Anhangfilter ist es Ihnen möglich, Regeln für Executables, also ausführbare Dateien aufzustellen.

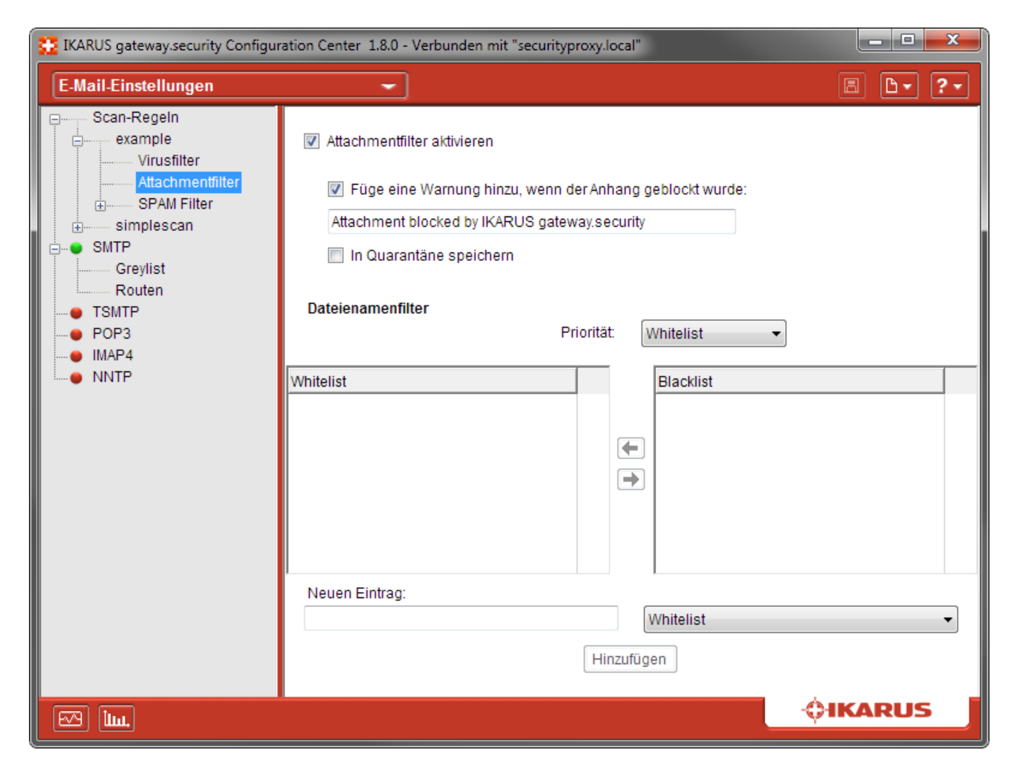


Abbildung 25: Attachmentfilter

Wert	Beschreibung
Attachmentfilter aktivieren	Diese Checkbox bestimmt, ob der Anhangfilter aktiviert oder deaktiviert ist.
Füge eine Warnung hinzu, wenn der Anhang geblockt wurde	Dieser Text wird der E-Mail hinzugefügt, wenn eine ausführbare Datei gelöscht wurde.
In Quarantäne speichern	Ist diese Option aktiviert, werden die geblockten ausführbaren Dateien im Quarantäneverzeichnis des Servers gespeichert.

Tabelle 18: Attachmentfilter

Dateinamen-Filter

Der Dateinamenfilter erlaubt Ihnen die Definition für Dateinamen in White- und Blacklists. Dadurch ist es möglich, z.B. E-Mails mit bestimmten Dateien im Anhang immer zu akzeptieren bzw. immer zu blocken. Sie können einen neuen Eintrag hinzufügen, müssen jedoch immer definieren, ob dieser der White- oder der Blacklist zugeordnet wird. Indem Sie eine Priorisierung von entweder der Whitelist oder der Blacklist festlegen, wird bestimmt, welche Regel zuerst greift. Die jeweils höher priorisierte Liste overruled dadurch die niedriger priorisierte.

SPAM-Schutz



IKARUS gateway.security bietet auch einen äußerst effektiven SPAM-Filter. Dieser erlaubt Ihnen die Definition von Schwellwerten, ab wann ein E-Mail als möglicher SPAM und ab wann sie als SPAM einzustufen ist. Sie können festlegen, wie mit diesen E-Mails zu verfahren ist.

Für die Filterung von SPAM werden fix vorgegebene Regeln verwendet. Um einen wirkungsvollen SPAM-Schutz aufzubauen brauchen Sie diesen also lediglich aktivieren und festlegen, wie mit SPAM-Mails umgegangen werden soll.

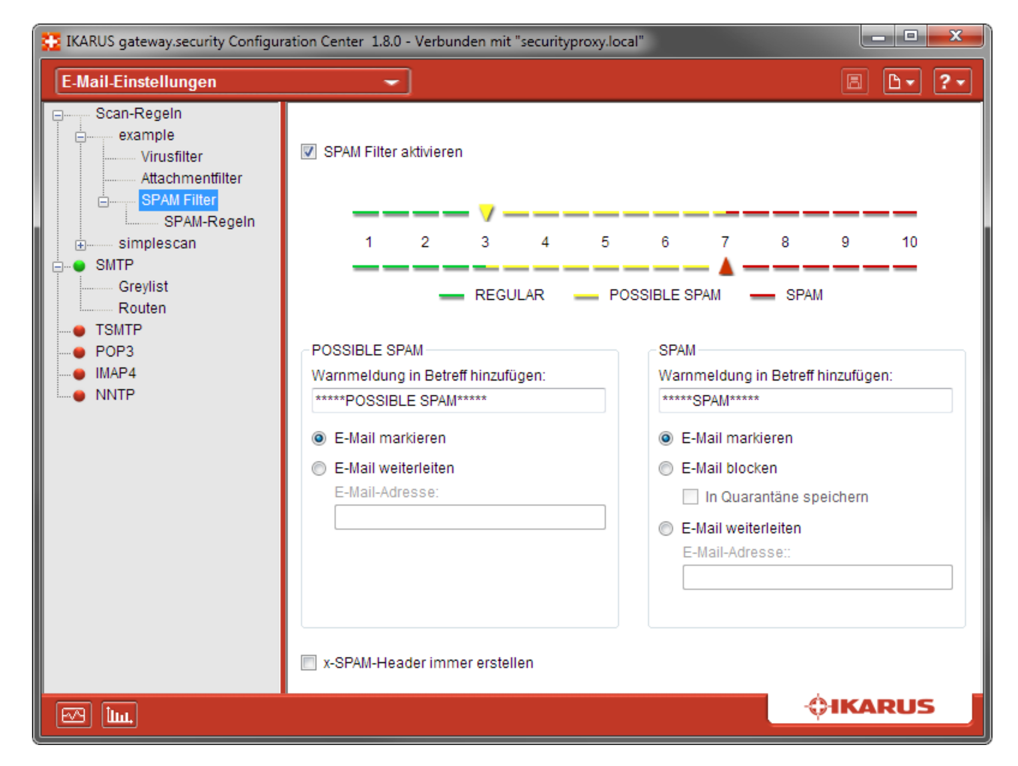


Abbildung 26: SPAM-Filter



Wert	Beschreibung
SPAM Filter aktivieren	Die Checkbox aktiviert bzw. deaktiviert den SPAM Filter.
SPAM-Regler	Mithilfe des SPAM-Reglers definieren Sie die Schwellwerte für possible SPAM und SPAM. Jede E-Mail erhält vom SPAM-Filter ein gewisses SPAM-Score, das sind Punkte, die für das Zutreffen bestimmter Eigenschaften vergeben werden (z.B. das Vorkommen des Wortes V1@gR@). Je mehr Punkte ein E-Mail also erhält, desto höher ist die Wahrscheinlichkeit, dass es sich dabei um SPAM handelt. Indem Sie die Schwellwerte definieren, legen Sie fest, ab wann ein E-Mail als möglicherweise verdächtig bzw. ab wann sie als SPAM eingestuft wird. Bitte beachten Sie, dass je niedriger Sie den Schwellwert definieren, desto höher die Chance ist, dass reguläre E-Mails als SPAM klassifiziert werden. Umgekehrt ist es daher auch möglich, dass zu hoch eingestellte Schwellwerte eindeutige SPAM-Mails als HAM (reguläre E-Mails) klassifizieren.
Possible SPAM	
Warnmeldung in Betreff hinzufügen	Es kann ein Text definiert werden, der im Betreff der E-Mail hinzugefügt wird.
E-Mail markieren	Wurde ein E-Mail als possible SPAM klassifiziert, so wird es als „possible SPAM“ markiert.
E-Mail weiterleiten	Wurde ein E-Mail als possible SPAM klassifiziert, so wird es an die unten definierte E-Mail-Adresse weitergeleitet. Achtung: wird nur von SMTP unterstützt.
SPAM	
Warnmeldung in Betreff hinzufügen	Es kann ein Text definiert werden, der im Betreff der E-Mail hinzugefügt wird.
E-Mail markieren	Wurde ein E-Mail als SPAM klassifiziert, so wird es als „SPAM“ markiert.
E-Mail blocken	Ein als SPAM klassifiziertes E-Mail wird geblockt (es wird also nicht zugestellt). Achtung: wird nur von SMTP unterstützt.
E-Mail weiterleiten	Ein als SPAM klassifiziertes E-Mail wird an eine vordefinierte E-Mail-Adresse weitergeleitet. Achtung: wird nur von SMTP unterstützt.
x-SPAM-Header immer erstellen	Ist diese Option aktiviert, wird ausnahmslos ein x-SPAM-Header von **IKARUS gateway.security** in den E-Mail-Header eingetragen.

Tabelle 19: SPAM-Schutz

AntiSPAM-Regeln

Es ist möglich, neben der fix vorgegebenen SPAM-Regeln auch eigene zu definieren. **IKARUS gateway.security** bietet Ihnen eine Vielzahl von Optionen an, mit denen Sie Ihre Regeln festlegen können. Mit diesen Regeln können sie die von **IKARUS gateway.security** durchgeführte Filterungen übersteuern, also z.B. bestimmte E-Mails immer als SPAM klassifizieren lassen, auch wenn diese ansonsten als HAM durchgegangen wären.

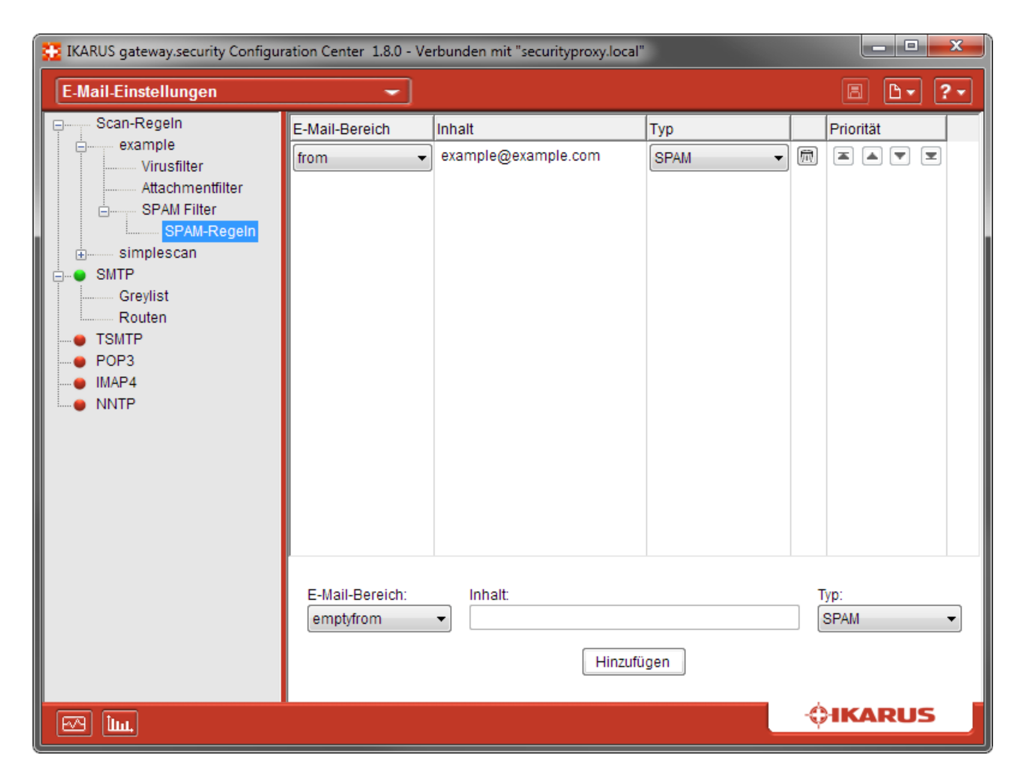


Abbildung 27: AntiSPAM-Regeln

Wert	Beschreibung
E-Mail-Bereich	Definiert den Teil der E-Mail, den Sie für Ihre Regel festlegen wollen. Für eine genaue Beschreibung siehe Tabelle „E-Mail-Bereich“
Inhalt	Abhängig vom E-Mail-Bereich können Sie hier einen bestimmten Inhalt definieren, dem der E-Mail-Bereich entsprechen muss, um zuzutreffen.
Typ	Hier legen Sie fest, ob ein E-Mail als SPAM, possible SPAM oder Regulär klassifiziert werden soll, falls die definierte Regel zutrifft.
Button „Hinzufügen“	Fügt die definierte Regel in der Liste mit höchster Priorität (oben) hinzu.

Tabelle 20: AntiSPAM-Regeln



Wert	Beschreibung
emptyfrom	From-Headereintrag ist leer
emptysubject	Subject-Headereintrag ist leer
emptyto	To-Headereintrag ist leer
envelop:from	SMTP-Envelope Empfänger ist <TO>
envelop:to	From-Headereintrag beinhaltet <FROM>
from	Der E-Mail-Body beinhaltet <TEXT>
mail:text	Der E-Mail-Body beinhaltet <TEXT>
nofromline	From-Headereintrag ist nicht vorhanden
nosubjectline	Subject-Headereintrag ist nicht vorhanden
notoline	To-Headereintrag ist nicht vorhanden
novalidaddrfrom	From-Headereintrag ist eine ungültige E-Mail-Adresse
novalidaddrto	To-Headereintrag ist eine ungültige E-Mail-Adresse
onlyhtmltext	Der E-Mail-Body ist nur HTML
subject	Subject-Headereintrag beinhaltet <SUBJECT>
to	To-Headereintrag enthält <TO>
toandfromequal	To-Headereintrag und From-Headereintrag sind gleich

Tabelle 21: E-Mail-Bereich - Aktionsfelder für AntiSPAM-Regeln

Jede dieser Regeln können Sie auf eine der folgenden drei Arten klassifizieren:

Wert	Beschreibung
SPAM	Ein E-Mail, auf welches diese Regel zutrifft, wird IMMER als SPAM klassifiziert
POSSIBLE	Ein E-Mail, auf welches die Regel zutrifft, wird IMMER als POSSIBLE SPAM klassifiziert
REGULAR	Ein E-Mail, auf welches diese Regel zutrifft wird als HAM, also als reguläres E-Mail klassifiziert

Tabelle 22: SPAM-Klassifizierungen

Falls mehrere Regeln auf ein E-Mail zutreffen, die sich gegenseitig ausschließen (also z.B. eine klassifiziertimmer als SPAM, die andere immer als REGULAR), dann greift die Priorisierung, d.h. jene Regel, die höher in der Liste angeführt ist, wird angewandt.

3.10.2 SMTP

IKARUS gateway.security erlaubt den Betrieb eines SMTP-Servers. Für diesen SMTP-Server können Routen definiert werden, welche anhand des Ursprungs bestimmen, wie eine SMTP-Verbindung weitergeleitet wird. Dies erlaubt vielseitige Anwendungsmöglichkeiten, wie **IKARUS gateway.security** für SMTP in Ihrem Netzwerk eingesetzt werden kann.

Darüber hinaus ist **IKARUS gateway.security** in der Lage, E-Mails, die via SMTP versandt werden, auf schad-



hafte Inhalte wie z.B. Viren zu überprüfen sowie SPAM zu filtern.

Konfiguration von SMTP

Die Konfigurationsmaske für SMTP erreichen Sie im **IKARUS gateway.security Configuration Center** über den Menüpunkt “E-Mail-Einstellungen“. In der Baumansicht wählen Sie SMTP aus.

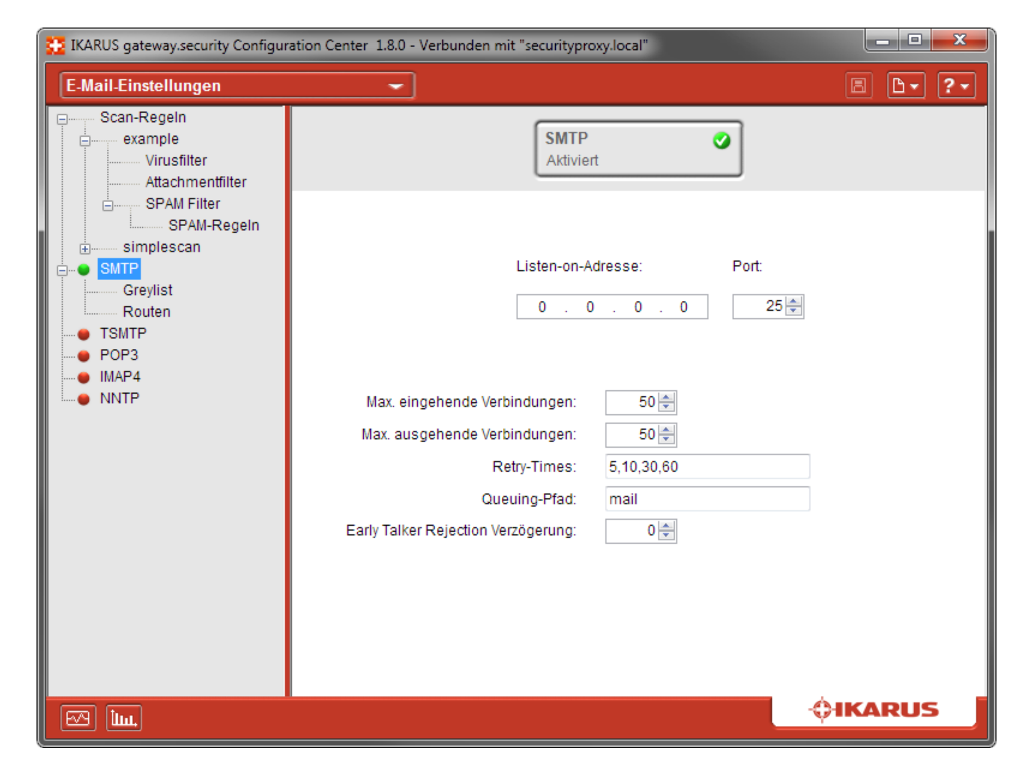


Abbildung 28: SMTP

Wert	Beschreibung
Button „SMTP“	Schaltet das SMTP-Service von **IKARUS gateway.security** ein oder aus. Achtung: Änderungen werden erst nach dem Speichern aktiv.
Listen-on-Adresse	Die IP-Adresse, an welcher das SMTP-Service betrieben wird. Wenn die IP-Adresse `0.0.0.0` angegeben wurde, versucht **IKARUS gateway.security** das Service an alle verfügbaren Netzwerk-Interfaces zu binden.
Port	Der Port, an welchem das SMTP-Service angeboten wird. Standardmäßig ist dies Port 25.
Max. eingehende Verbindungen	Die Anzahl der gleichzeitigen eingehenden SMTP-Verbindungen, die **IKARUS gateway.security** zulässt. Ist dieser Wert überschritten, wird eine Fehlermeldung an jene Verbindungen geschickt, die über dem Limit ist.
Max. ausgehende Verbindungen	Die Anzahl der gleichzeitigen ausgehenden Verbindungen, die **IKARUS gateway.security** beim Versenden von E-Mails aufbaut.
Retry-Times	Bestimmt die Anzahl und den Zeitpunkt von erneuten Zustellversuchen, falls die ursprüngliche Zustellung nicht erfolgreich war. Beispielsweise bestimmen die Werte 5, 10, 30, 60 dass der erste erneute Zustellversuch nach 5, der zweite nach 10, der dritte nach 30 und der vierte nach 60 Minuten durchgeführt wird.
Queuing-Pfad	Der Pfad, in welchem E-Mails zwischengespeichert werden. Dieser ist relativ zum Installationsverzeichnis von **IKARUS gateway.security**.
Early Talker Rejection Verzögerung	Die Anzahl der Sekunden, die das SMTP-Service warten soll, bevor das SMTP-Banner geschickt wird. Hiermit lassen sich Spam-Bots abblocken, die SMTP-unkonform Daten schicken, bevor vom Mailserver das Banner geschickt wurde, um die Bereitschaft zu signalisieren.

Tabelle 23: SMTP-Einstellungen

Greylisting

Um das Ausmaß zugestellter SPAM-Mails einzugrenzen, können Sie Greylisting aktivieren.

Details zur Verwendung des Greylistings finden sie im Abschnitt 4.3

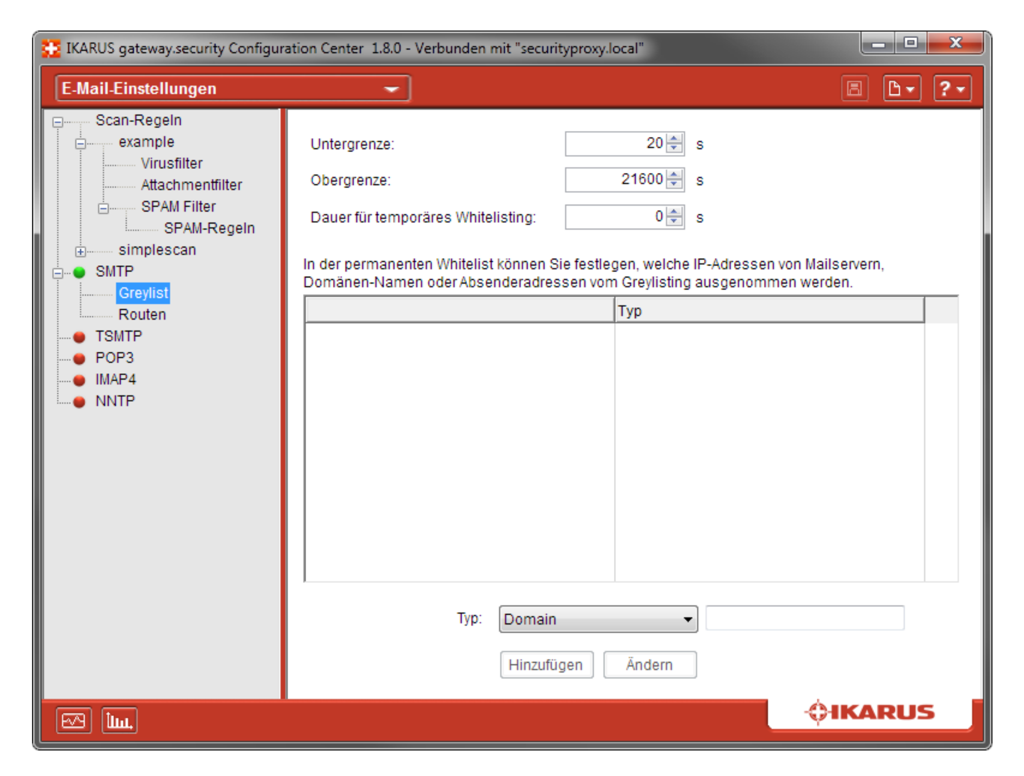


Abbildung 29: SMTP - Greylisting

Wert	Beschreibung
Untergrenze	Die Zeit die mindestens verstreichen muss, bis das gegreylistete Mail akzeptiert wird.
Obergrenze	Die Zeit die maximal verstreichen darf, damit das gegreylistete Mail akzeptiert wird.
Dauer für temporäres Whitelisting	Ist dieser Wert ungleich Null und vorhanden, so ist temporäres Whitelisting aktiviert. In die Whitelist aufgenommene Einträge bleiben für den angegebenen Zeitraum gültig und werden danach erneut dem Greylisting unterzogen.
Permanente Whitelist	Hier können Sie festlegen, ob IP-Adressen von Mailservern, Domänen-Namen oder Absenderadressen vom Greylisting ausgenommen werden.

Tabelle 24: SMTP - Greylisting

Definieren von Routen

Um den SMTP-Server zu betreiben, müssen Sie Routen definieren, damit **IKARUS gateway.security** in der Lage ist, eingehende SMTP-Verbindungen richtig zu bearbeiten. Sie können beliebig viele Routen definieren. Die hierbei aufgestellten Regeln werden in einer Liste angeführt und nach Priorität abgearbeitet, wobei die Priorität von der Position in der Liste definiert wird: je höher die Position in der Liste, desto höher die Priorität.

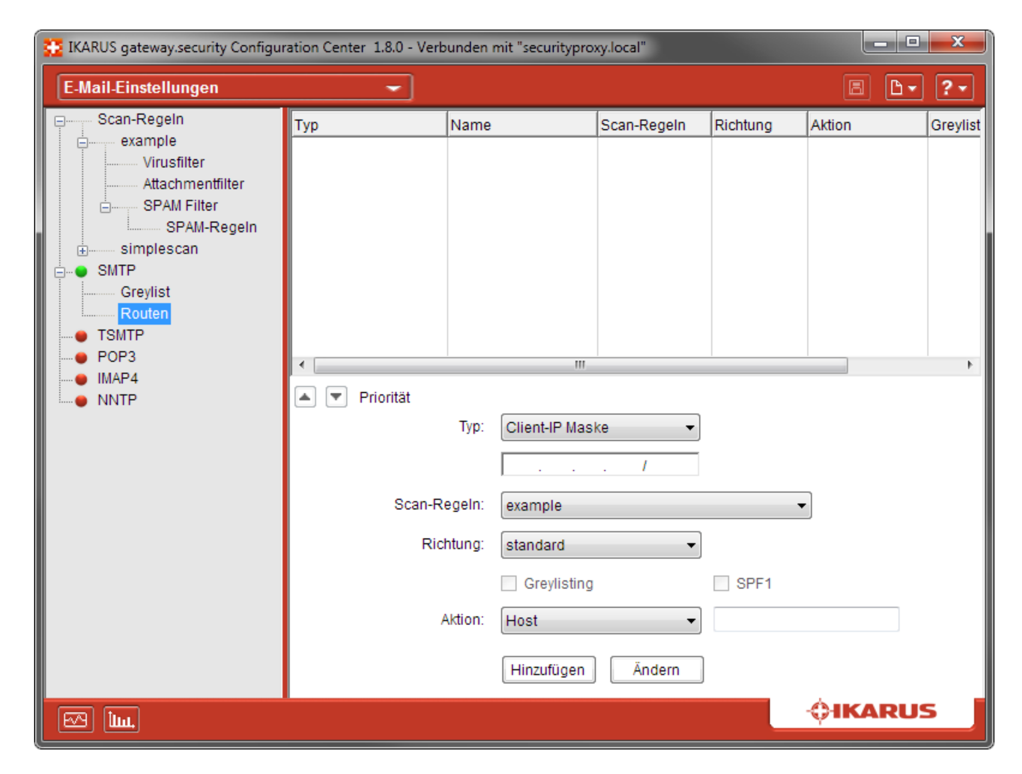


Abbildung 30: SMTP-Routen

Wert	Beschreibung
Typ	Bestimmt den Typ der Route. Es können Routen basierend auf der IP-Adresse des Senders (bzw. des IP-Netzes), einer Liste von Ziel-Domänen bzw. Ziel-E-Mail-Adressen, LDAP* oder einer Mailbox-Datei definiert werden.
Scan-Regeln	Für jede Route muss die anzuwendende Scan-Regel definiert werden.
Richtung	Legt fest ob die Route inbound, outbound oder standard ist.
Greylisting	Bei Inbound-Routen kann Greylisting aktiviert werden.
SPF1	Bei Inbound-Routen kann SPF aktiviert werden.
Aktion	Die Aktion bestimmt, wie E-Mails geroutet werden. Die möglichen Aktionen sind Host (hierbei kann sowohl die IP-Adresse des Ziel-hosts als auch ein auflösbarer Rechnername angegeben werden) und MX (hier wird versucht, abhängig vom Empfänger im SMTP-Envelope an den vom DNS vordefinierten Mail Exchanger der Zieldomäne zuzustellen).

Tabelle 25: Definition von SMTP-Routen

* Mit Hilfe der LDAP-Funktionalität können nur im Active Directory angelegte Mailboxen für eine Route verwendet werden. Der LDAP-String muss in folgendem Format eingegeben werden:

```
ldap[s]://<user-cn/dc>:<passwort>@<domain-controller>/<query>
```



Hier ist ein Beispiel eines gültigen LDAP-Strings für „readonlyuser@test.local“ mit Passwort „mypassword“ auf dem Domain-Controller „dc.test.local“:

```
ldaps://CN=readonlyuser,CN=Users,dc=test,dc=local:mypassword@dc.test.local/DC=test,
DC=local?proxyaddresses?sub?(proxyaddresses=SMTP:*)
```

3.10.3 TSMTP - der transparente SMTP Proxy

Zusätzlich zu der SMTP-Funktionalität von **IKARUS gateway.security** ist es auch möglich, einen SMTP-Proxy zu betreiben. Hierbei wird die gesamte Kommunikation zwischen einem Client und einem SMTP-Server über **IKARUS gateway.security** weitergeleitet. **IKARUS gateway.security** speichert dabei keinerlei E-Mails. Auch hier ist es möglich, auf diese Weise übermittelte E-Mails auf Viren oder SPAM zu prüfen.

Unter Linux ist es möglich, den SMTP Proxy im volltransparenten Modus zu betreiben. Richtig definierte Routen und entsprechende Konfiguration von iptables vorausgesetzt ermöglicht dies das Scannen von E-Mails ohne entsprechende Konfiguration auf den Mailclients in Ihrem Netzwerk.

Unter Windows wird der transparente Modus derzeit nicht angeboten. Sie können anstatt dessen einen fix vorgegebenen SMTP-Ziel-Server angeben, zu welchem der am Proxy eingehende SMTP Traffic weitergeleitet wird.

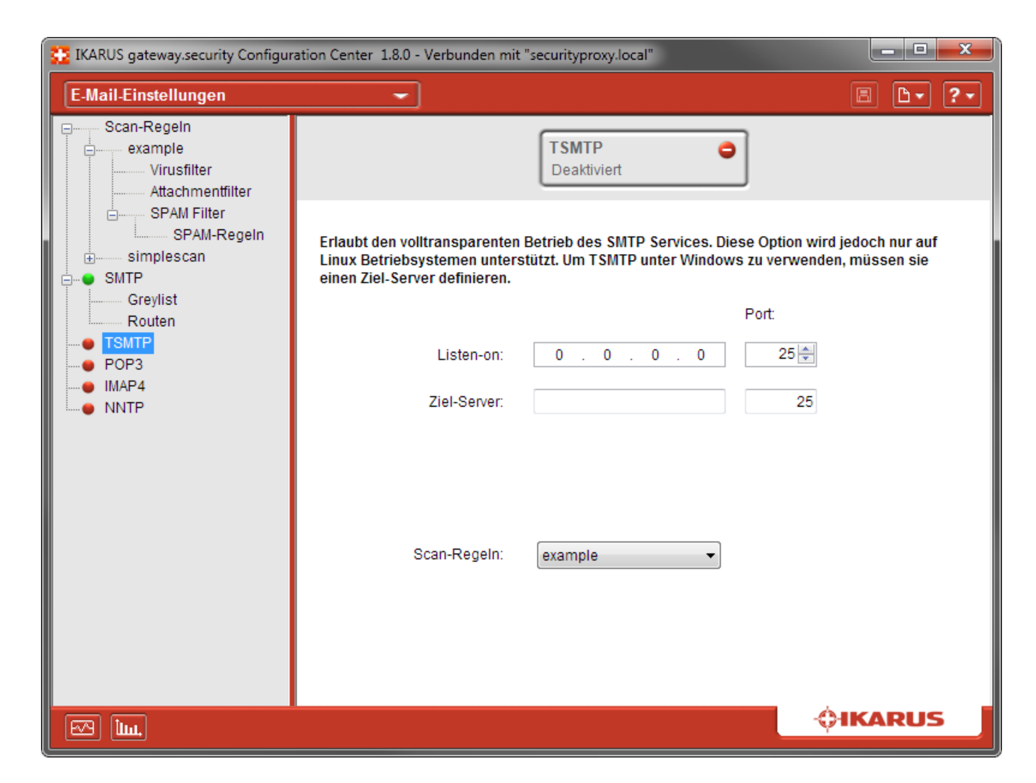


Abbildung 31: TSMTP

Wert	Beschreibung
Button „TSMTP“	Schaltet das TSMTP-Service von **IKARUS gateway.security** ein oder aus. Achtung: Änderungen werden erst nach dem Speichern aktiv.
Listen-on-Adresse	Die IP-Adresse, an welcher das TSMTP-Service betrieben wird. Wenn die IP-Adresse 0.0.0.0 angegeben wurde, versucht **IKARUS gateway.security**, das Service an allen verfügbaren Netzwerk-Interfaces zu binden.
Port	Der Port, an welchem das TSMTP-Service angeboten wird. Standardmäßig ist dies Port 25.
Ziel-Server und Port	Alternativ verwendeter NNTP-Server, der verwendet wird, wenn kein NNTP-Server im Usernamen angegeben wird.
Scan-Regeln	Jene Scan-Regel, welche für TSMTP angewandt werden soll.

Tabelle 26: TSMTP-Einstellungen

3.10.4 POP3

IKARUS gateway.security erlaubt das Betreiben eines POP3-Proxy. Dies ermöglicht den Proxybetrieb von unverschlüsselter POP3-Kommunikation. So ist es z.B. möglich, dass Clients in Ihrem Netzwerk Nachrichten von einem POP3-Server im Internet abfragen und die abgerufenen Nachrichten dennoch auf Viren und/oder SPAM gescannt werden können.

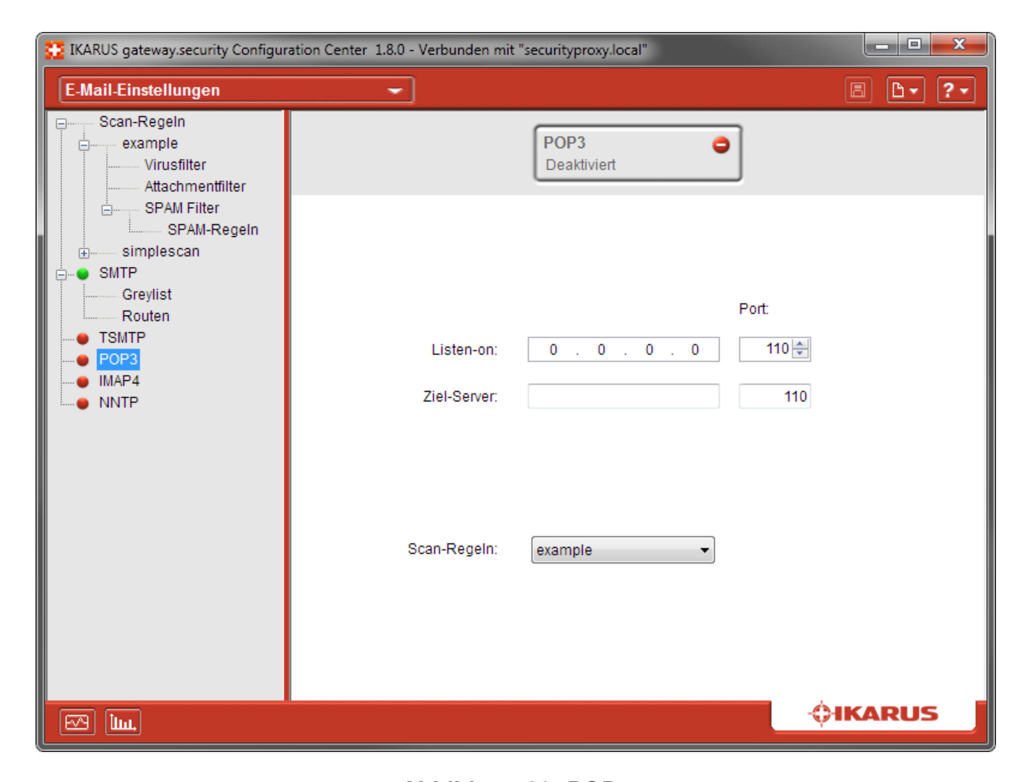


Abbildung 32: POP3

Wert	Beschreibung
Button „POP3“	Schaltet den POP3-Proxy von **IKARUS gateway.security** ein oder aus. Achtung: Änderungen werden erst nach dem Speichern aktiv.
Listen-on-Adresse	Die IP-Adresse, an welcher der POP3-Proxy betrieben wird. Wenn die IP-Adresse 0.0.0.0 angegeben wurde, versucht **IKARUS gateway.security**, das Service an allen verfügbaren Netzwerk-Interfaces zu binden.
Port	Der Port, an welchem der POP3-Proxy lauscht. Standardmäßig ist dies Port 110.
Ziel-Server und Port	Alternativ verwendeter POP3-Server, der verwendet wird, wenn kein POP3-Server im Usernamen angegeben wird.
Scan-Regeln	Die für den POP3-Proxy anzuwendenden Scan-Regeln.

Tabelle 27: POP3-Einstellungen

Konfiguration von E-Mail-Clients

Wenn Sie den POP3-Proxy mit Ihren E-Mail-Clients verwenden wollen, müssen geringfügige Anpassungen in deren Konfiguration durchgeführt werden:

POP3-Server: Anstelle des POP3-Servers geben Sie die IP-Adresse bzw. den auflösbaren Namen von **IKARUS gateway.security** an, damit sich der Mail-Client bei POP3-Abfragen über diesen verbindet.

Username: Ergänzen Sie den Usernamen der POP3 Mailbox mit einem @ und dem Computernamen/der IP-Adresse des POP3-Severs

Beispiel: Sie haben eine Mailbox für die E-Mail-Adresse max.mustermann@example.com mit dem Usernamen max auf dem POP3-Server pop.example.com. Damit **IKARUS gateway.security** E-Mail-Nachrichten von diesem POP3-Server abruft, ändern sie den Usernamen von max auf max@pop.example.com

Alternativ kann ein Default-Server in **IKARUS gateway.security** definiert werden, an welchen POP3 Requests weitergeleitet werden. In diesem Fall brauchen Sie die oben beschriebene Anpassung des User-E-Mail Accounts nicht durchführen. Allerdings funktioniert der POP3-Proxydienst in diesem Fall genau mit nur diesem einen POP3-Server.

3.10.5 IMAP4

IKARUS gateway.security erlaubt das Betreiben eines IMAP4 Proxy. Dies ermöglicht den Proxybetrieb von unverschlüsselter IMAP4-Kommunikation. So ist es z.B. möglich, dass Clients in Ihrem Netzwerk Nachrichten von einem IMAP4-Server im Internet abfragen und die abgerufenen Messages dennoch auf Viren und/oder SPAM gescannt werden können.

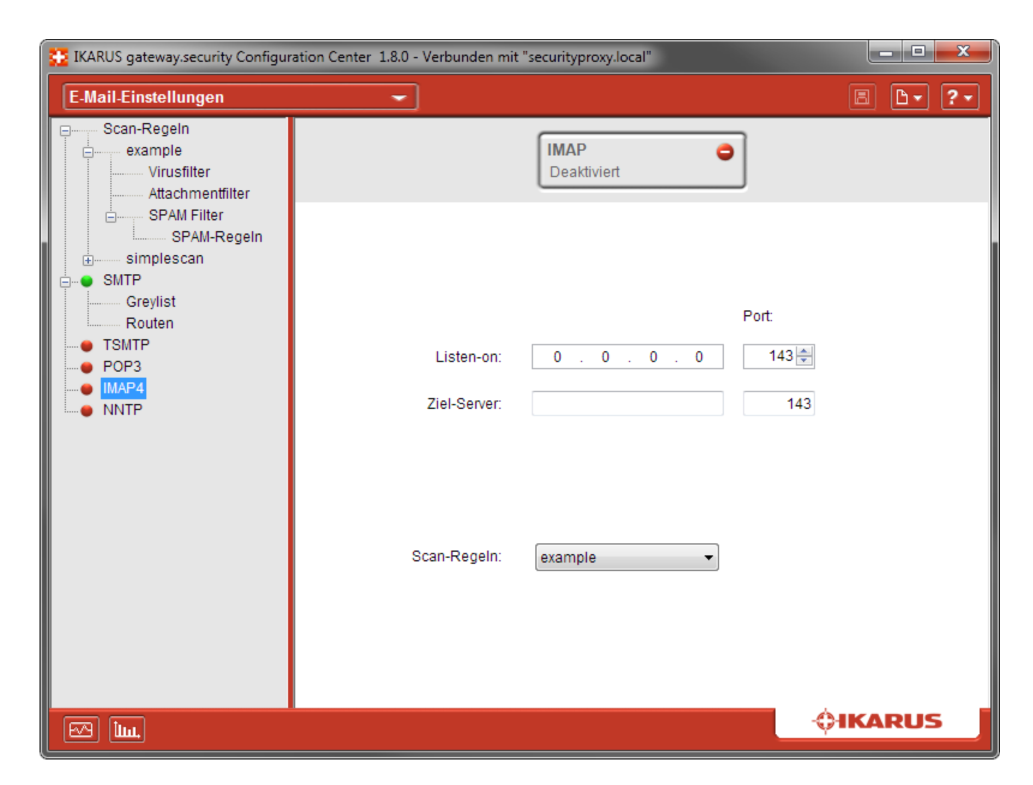


Abbildung 33: IMAP4

Wert	Beschreibung
Button „IMAP4“	Schaltet den IMAP4-Proxy von **IKARUS gateway.security** ein oder aus. Achtung: Änderungen werden erst nach dem Speichern und Neustart des **IKARUS gateway.security** Dienstes aktiv.
Listen-on-Adresse	Die IP-Adresse, an welcher der IMAP4-Proxy betrieben wird. Wenn die IP-Adresse 0.0.0.0 angegeben wurde, versucht **IKARUS gateway.security**, das Service an allen verfügbaren Netzwerk-Interfaces zu binden.
Port	Der Port, an welchem der IMAP4-Proxy lauscht. Standardmäßig ist dies Port 143.
Ziel-Server und Port	Alternativ verwendeter IMAP4-Server, der verwendet wird, wenn kein IMAP4-Server im Usernamen angegeben wird.
Scan-Regeln	Die für den IMAP4-Proxy anzuwendenden Scan-Regeln.

Tabelle 28: IMAP4-Einstellungen

Konfiguration von E-Mail-Clients

Wenn Sie den IMAP4-Proxy mit Ihren E-Mail-Clients verwenden wollen, müssen geringfügige Anpassungen in deren Konfiguration durchgeführt werden:

IMAP-Server: anstelle des IMAP4-Servers geben Sie die IP-Adresse bzw. den auflösbaren Namen von **IKARUS gateway.security** an, damit sich der E-Mail-Client bei IMAP4-Abfragen über diesen verbindet.



Username: Ergänzen Sie den Usernamen der IMAP4 Mailbox mit einem @ und dem Computernamen/der IP-Adresse des IMAP4-Severs.

Beispiel: Sie haben eine Mailbox für die E-Mail-Adresse max.mustermann@example.com mit dem Usernamen max auf dem IMAP4-Server imap.example.com. Damit **IKARUS gateway.security** E-Mail-Nachrichten von diesem IMAP4-Server abruft, ändern Sie den Usernamen von max auf max@imap.example.com.

3.10.6 NNTP

Neben den Mailprotokollen SMTP, POP3 und IMAP bietet **IKARUS gateway.security** auch die Möglichkeit der Übertragung des Network News Transfer Protocols. Wie bei den anderen Mailprotokollen können Sie Scanregeln für dieses Protokoll erstellen und anwenden.

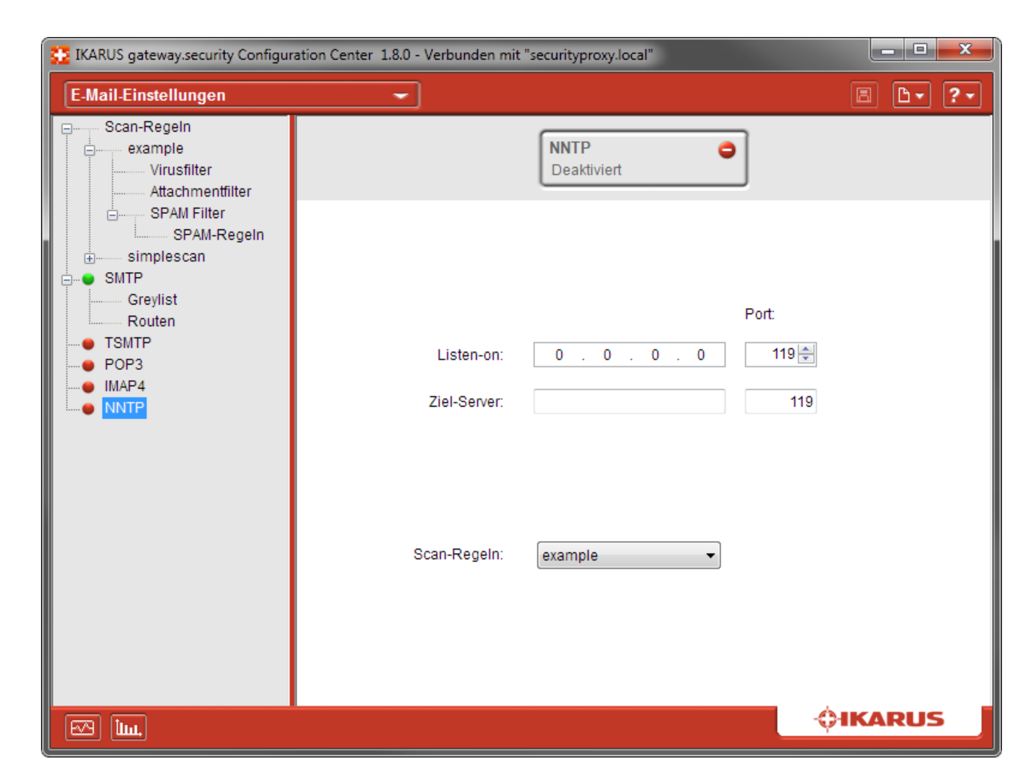


Abbildung 34: NNTP

Wert	Beschreibung
Button „NNTP“	Schaltet den NNTP-Proxy von **IKARUS gateway.security** ein oder aus. Achtung: Änderungen werden erst nach dem Speichern aktiv.
Listen-on-Adresse	Die IP-Adresse, an welcher der NNTP-Proxy betrieben wird. Wenn die IP-Adresse 0.0.0.0 angegeben wurde, versucht **IKARUS gateway.security**, das Service an allen verfügbaren Netzwerk-Interfaces zu binden.
Listen-on-Port	Der Port, an welchem der NNTP-Proxy lauscht. Standardmäßig ist dies Port 119.
Ziel-Server und Port	Alternativ verwendeter NNTP-Server, der verwendet wird, wenn kein NNTP-Server im Usernamen angegeben wird.
Scan-Regeln	Die für den NNTP-Proxy anzuwendenden Scan-Regeln.

Tabelle 29: NNTP-Einstellungen

3.11 Eigenes Netzwerk

IKARUS gateway.security erlaubt Ihnen die Festlegung von Netzwerken mittels Erstellung von Netzwerk-Listen. Hier können Sie einzelne Rechneradressen oder komplette Netzwerke zu einer logischen Gruppe zusammenfassen, die Sie dann bei der Definition von Proxy-Settings verwenden können.

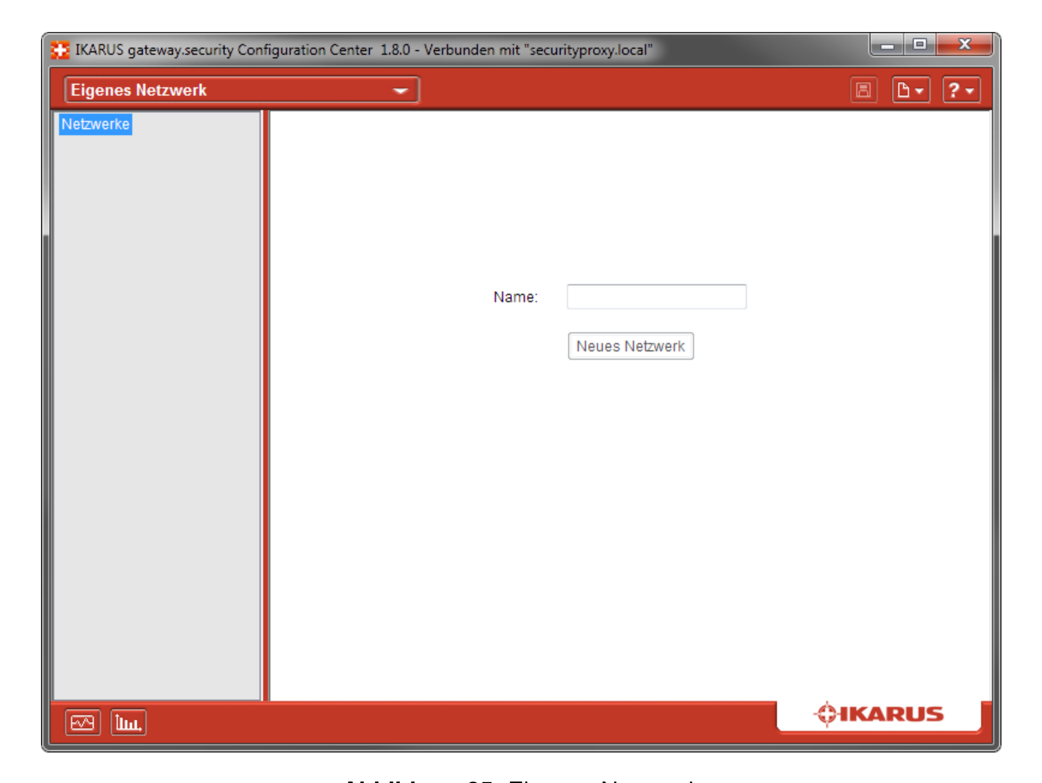


Abbildung 35: Eigenes Netzwerk

Wert	Beschreibung
Name	Der Name für das Netzwerk. Erlaubt sind alphanumerische Zeichen sowie -,_ und .
IP-Adresse/Subnetmaske	Eine IPv4 Adresse samt zugehöriger Subnetzmaske. Um einzelne IP-Adressen zu definieren, müssen Sie als Subnetzmaske /32 definieren (32 bit Hostadresse, 0 bit Netzwerkhosts).
Button „Neues Netzwerk“	Erstellt eine neue Netzwerk-Liste.
Button „Netzwerk löschen“	Löscht die ausgewählten Netzwerk-Liste. Achtung: Wird eine Netzwerk-Liste in einer Access-Liste verwendet ist ein Löschen nicht möglich.

Tabelle 30: Eigenes Netzwerk

3.12 Clustering

Mehrere Installationen von **IKARUS gateway.security** können zu einem Cluster zusammengefasst werden. Die Konfiguration wird dadurch unter allen Proxies im Cluster synchronisiert. Beachten Sie, dass ein Cluster aus mindestens zwei Instanzen von **IKARUS gateway.security** bestehen muss. Dabei ist es unerheblich, auf welchem Betriebssystem die einzelnen Proxyinstanzen installiert sind. So ist es auch möglich, einen Proxy auf Windows und einen anderen auf Linux laufen zu lassen.

Wichtig: Es muss immer die IP-Adresse des eigenen Proxies eingetragen sein, um einen Cluster zu bilden. Bitte beachten Sie, dass der Port für den Remotemanager auf dem Standartwert (15639) belassen werden muss, wenn das Clustering aktiviert ist, da ansonsten der Datenaustausch zwischen den Proxyservern im Cluster nicht möglich ist.

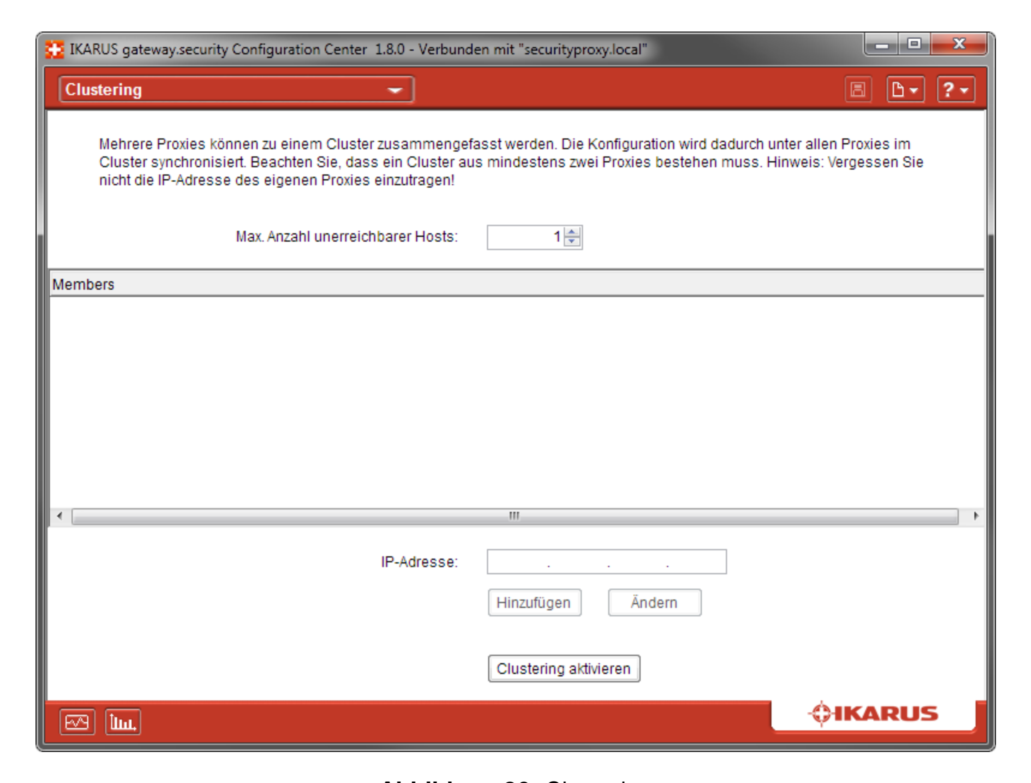


Abbildung 36: Clustering



Wert	Beschreibung
Max. Anzahl unerreichbarer Hosts	Die Anzahl der Hosts im Cluster, die maximal unerreichbar bzw. ausgefallen sein dürfen. Ist diese Zahl erreicht, ist ein Softstop der verbleibenden **IKARUS gateway.security** Instanz nicht mehr möglich.
Mitglieder	Eine Auflistung der **IKARUS gateway.security** Instanzen, die sich in diesem Cluster befinden.
IP-Adresse	Die IP-Adresse der **IKARUS gateway.security** Instanz, die dem Cluster hinzugefügt werden soll.
Button „Hinzufügen“	Durch Betätigen dieses Buttons wird die erfasste IP-Adresse zu der Liste der Proxyserver hinzugefügt.
Button „Ändern“	Ermöglicht die Änderung einer bereits erfassten IP-Adresse.
Button „Clustering aktivieren“ / „Clustering deaktivieren“	Durch Betätigung dieses Buttons wird das Clustering aktiviert bzw. deaktiviert. Achtung: Änderungen werden erst nach dem Speichern wirksam.

Tabelle 31: Clustering

3.13 WCCP

In einem Netzwerk mit mehreren Instanzen von **IKARUS gateway.security** kann über WCCP die Weiterleitung der IP-Pakete konfiguriert werden.

Eine der **IKARUS gateway.security**-Instanzen muss als *Designated Web Cache* konfiguriert werden. Diese Instanz ist für die Aufteilung der eingehenden Pakete auf alle **IKARUS gateway.security**-Instanzen zuständig.

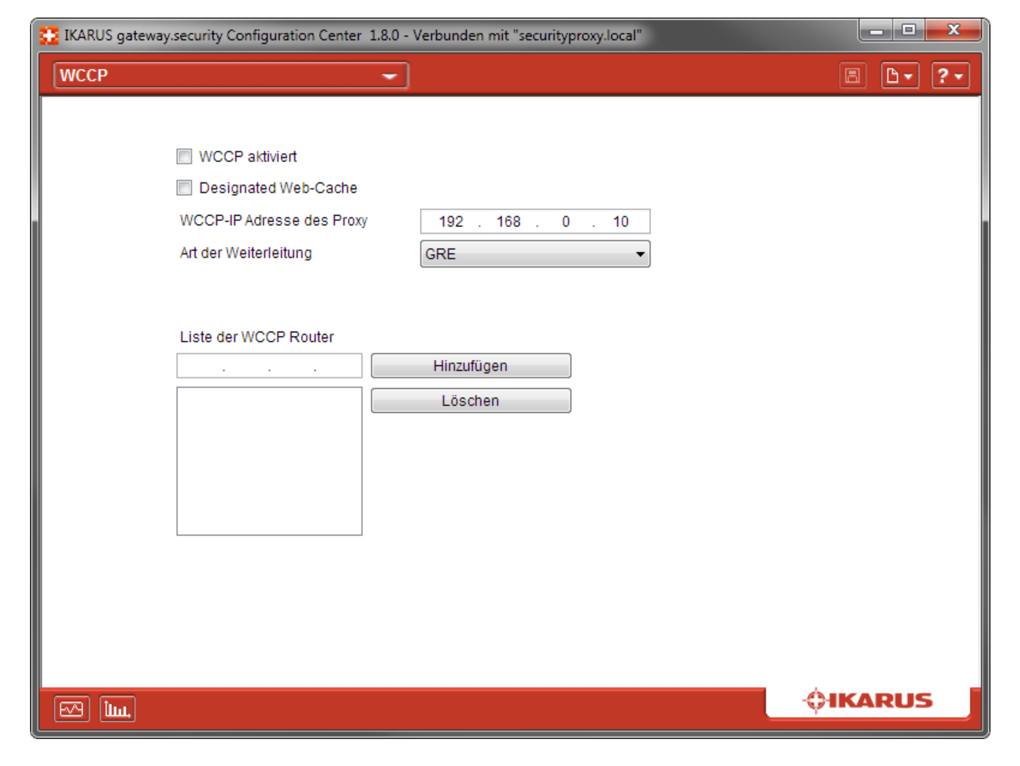


Abbildung 37: WCCP

Wert	Beschreibung
WCCP aktiviert	Aktiviert/deaktiviert WCCP.
Designated Web-Cache	Konfiguriert die **IKARUS gateway.security**-Instanz als Master. Dieser ist für die Aufteilung der Pakete auf alle Instanzen zuständig.
WCCP-IP Adresse des Proxy	IP-Adresse des Proxys aus Sicht des Routers. Diese muss konfiguriert werden, damit IP-Adresse der Verbindung und bekanntgegebene IP-Adresse übereinstimmen.
Art der Weiterleitung	**GRE:** Pakete werden in GRE gekapselt zum Proxy geschickt **Layer2:** Pakete werden mittels Umschreiben der Ziel-MAC-Adresse an den Proxy geleitet
Liste der WCCP Router	Liste der WCCP-Router, mit denen eine Verbindung aufgebaut werden soll

Tabelle 32: WCCP

3.14 Reporting

Mit **IKARUS gateway.security** können einfach grafische Berichte erstellt werden, um Internetaktivität und Mailaufkommen nach verschiedenen Kriterien ausgewertet darzustellen.

Die Seite „Reporting“ erlaubt es, Reports zu definieren, die im Reporting-Anzeigedialog angesehen werden bzw. automatisiert verschickt werden können. Außerdem können Datenkbankoptionen verwaltet werden.

Hierfür ist die Seite in vier Bereiche aufgeteilt:

- Globale Reporting-Einstellungen
- Automatisiert Reports erstellen und verschicken
- Reports mit Hilfe von Templates erstellen
- Vorhandene Reports bearbeiten

3.14.1 Globale Einstellungen

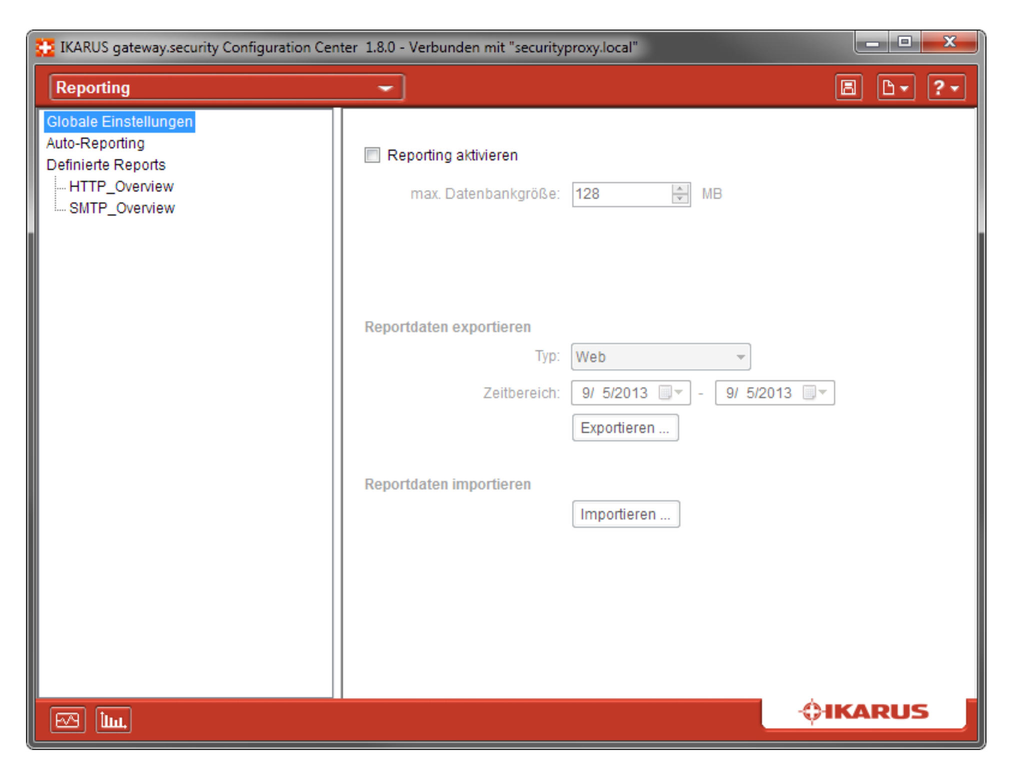


Abbildung 38: Reporting: Globale Einstellungen

Wert	Beschreibung
Reporting aktivieren	Aktiviert das Reporting für **IKARUS gateway.security**. Ist das Reporting deaktiviert, werden keine Daten geloggt; wird es reaktiviert, wird die ggf. bereits vorhandene Datenbank weiter befüllt, wodurch es zu zeitlichen Lücken bei den Daten kommen kann.
Max. Datenbankgröße	Legt die Größe der Datenbank auf der Platte in MB fest. Wird die Größe überschritten, werden jeweils die ersten 5 Prozent der Daten gelöscht. *
Datenbank-Pfad	Legt fest, wo die Datenbank abgelegt werden soll.
Reportdaten exportieren	
Typ	Bestimmt, welche Daten exportiert werden sollen.
Zeitbereich	Bestimmt den Zeitraum, aus dem die Daten exportiert werden sollen.
Button „Exportieren ...“	Öffnet einen Speicherdialog und speichert die exportierten Daten im CSV-Format in die ausgewählte Datei.
Reportdaten importieren	
Button „Importieren ...“	Importiert ein File im CSV-Format (wenn wie beim Exportieren formatiert) in die Datenbank.

Tabelle 33: Reporting: Globale Einstellungen



* Zum Löschen der ersten fünf Prozent der Datenbank wird das Einfügedatum herangezogen, nicht das Datum des Eintrags selbst. Das bedeutet, dass importierte Daten erst zuletzt gelöscht werden, was unter Umständen dazu führen kann, dass durch das automatische Löschen Lücken entstehen, wenn importierte CSV-Dateien alte Datensätze enthalten.

3.14.2 Auto-Reporting

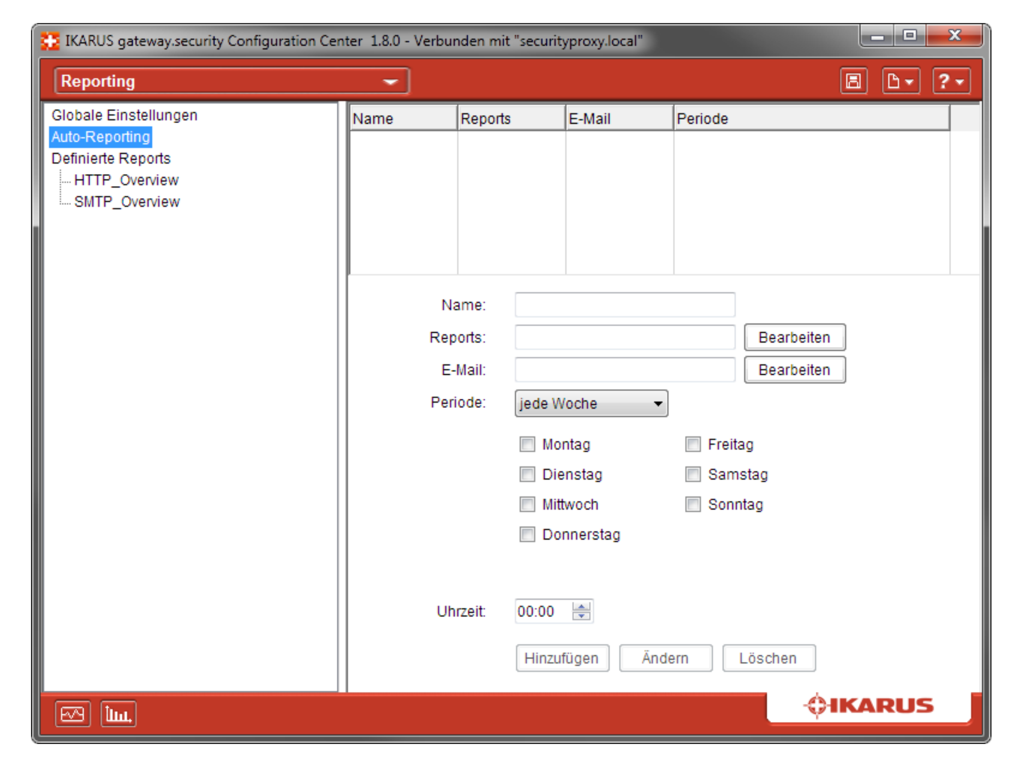


Abbildung 39: Reporting: Auto-Reporting



Wert	Beschreibung
Name	Der Name, unter welchem der Auto-Reporting-Eintrag gespeichert wird.
Reports	Eine Liste an Reports, die automatisiert erstellt und verschickt werden sollen. Die Reports können über ein eigenes Dialogfeld ausgewählt werden, das über die Schaltfläche „Bearbeiten“ erreichbar ist.
E-Mail	Empfänger der automatisiert erstellten Reports. Über die Schaltfläche „Bearbeiten“ öffnet sich ein Dialogfeld, über welches E-Mail-Adressen eingegeben werden können.
Periode	Hier kann eingestellt werden, ob Tage pro Woche oder pro Monat ausgewählt werden sollen.
Wochentage/Monatstage	Je nach Perioden-Einstellung können hier Wochentage (Montag-Sonntag) oder Tage eines Monats (1-31) eingestellt werden. Achtung: Es wird kein Report versendet, wenn einer der Tage 29-31 ausgewählt ist und der aktuelle Monat diesen Tag nicht beinhaltet.
Uhrzeit	Uhrzeit, zu der der Report verschickt werden soll.
Button „Hinzufügen“	Fügt einen neuen Eintrag mit den angegebenen Werten hinzu.
Button „Ändern“	Überschreibt den selektierten Auto-Reporting-Eintrag mit den angegebenen Werten.
Button „Löschen“	Löscht den ausgewählten Auto-Reporting-Eintrag.

Tabelle 34: Reporting: Auto-Reporting



3.14.3 Neuen Report erstellen

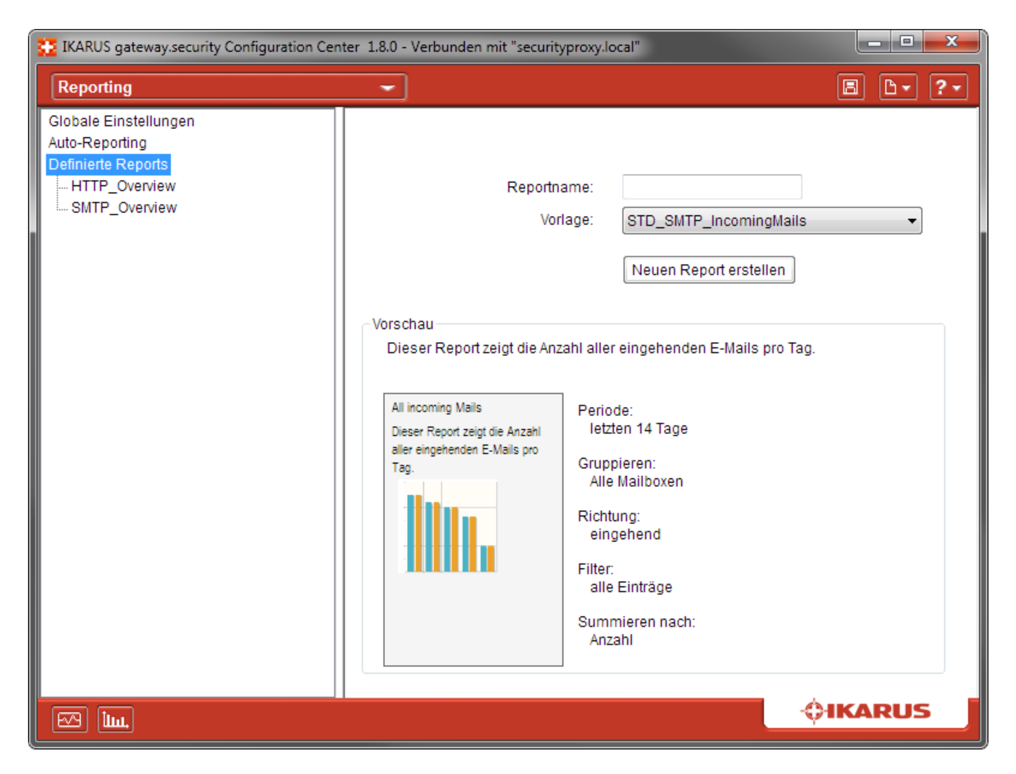


Abbildung 40: Reporting: Neuen Report erstellen

Wert	Beschreibung
Reportname	Legt den Namen des zu erstellenden Reports fest.
Vorlage	Hier kann aus einer Liste von Vorlagen gewählt werden, welche Art von Report man haben will. Der neue Report wird dann mit den entsprechenden Voreinstellungen erstellt, kann aber anschließend den eigenen Wünschen entsprechend angepasst werden.
Button „Neuen Report erstellen“	Erstellt den neuen Report und fügt ihn in der Liste als auch im Reporting-Anzeigedialog hinzu.
Vorschau	Hier wird ein Überblick über den Reporttyp und die voreingestellten Filteroptionen für die ausgewählte Vorlage gegeben.

Tabelle 35: Reporting: Neuen Report erstellen



3.14.4 Definierte Reports

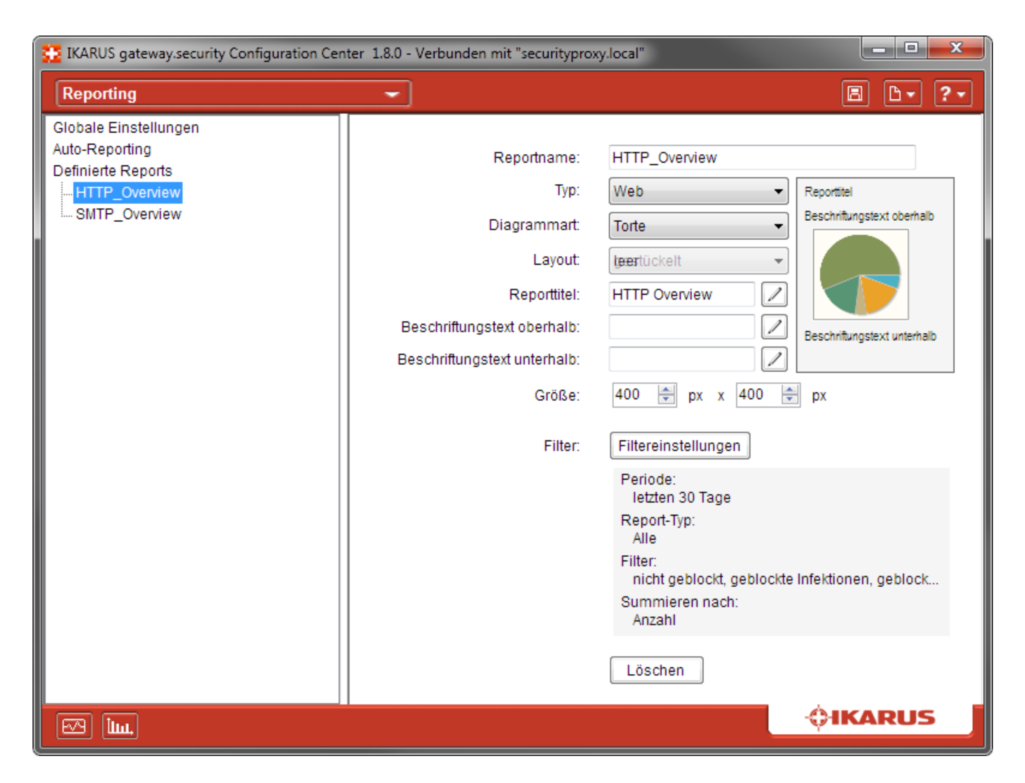


Abbildung 41: Reporting: Definierte Reports

Wert	Beschreibung
Reportname	Der Name, unter welchem der Report gespeichert wurde.
Typ	Der Typ des Reports (Web oder Mail).
Diagrammart	Die Darstellung der Daten mittels Balken-, Torten- oder Liniendiagramm oder auch in einer Tabelle
Layout	Der Layouttyp des Diagramms, er ist abhängig von der gewählten Diagrammart (z.B. gefüllte Balken).
Reporttitel	Der Titel, der als Überschrift des Reports dienen soll.
Beschriftungstext oberhalb	Erklärungstext, der direkt über dem Report angezeigt wird.
Beschriftungstext unterhalb	Erklärungstext, der unter dem Report angezeigt wird.
Button „Edit“	Hiermit wird ein kleines Dialogfenster geöffnet, in dem der jeweilige Text besser bearbeitet werden kann.
Größe	Die Größe des Reports – Breite mal Höhe – in Pixel.
Filter – Button „Filtereinstellungen“	Hier wird ein Dialog geöffnet, in welchem die Filtereinstellungen für den ausgewählten Reporttyp bearbeitet werden können. Das darunterliegende Feld fasst die getroffenen Filtereinstellungen zusammen.
Button „Löschen“	Löscht den ausgewählten Report.

Tabelle 36: Reporting: Definierte Reports



Erst nach dem erfolgreichen Speichervorgang sind die neu erstellten Reports bzw. Änderungen bereits vorhandener Reports im Anzeigedialog verfügbar, da das Sammeln und Auswerten der Daten Proxy-seitig geschieht.

Diagrammarten und Layouttypen

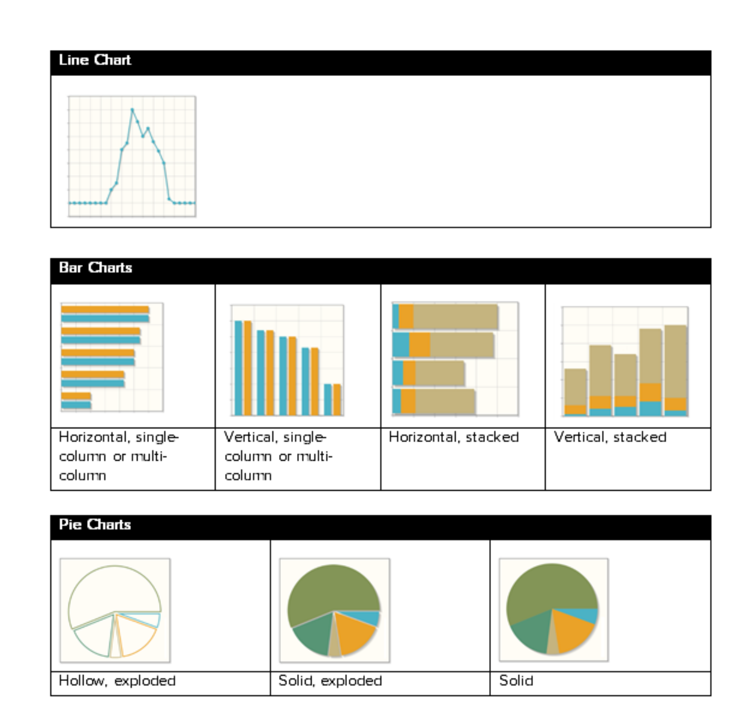


Abbildung 42: Reporting: Diagrammarten und Layouttypen

Filtereinstellungen für Typ Web

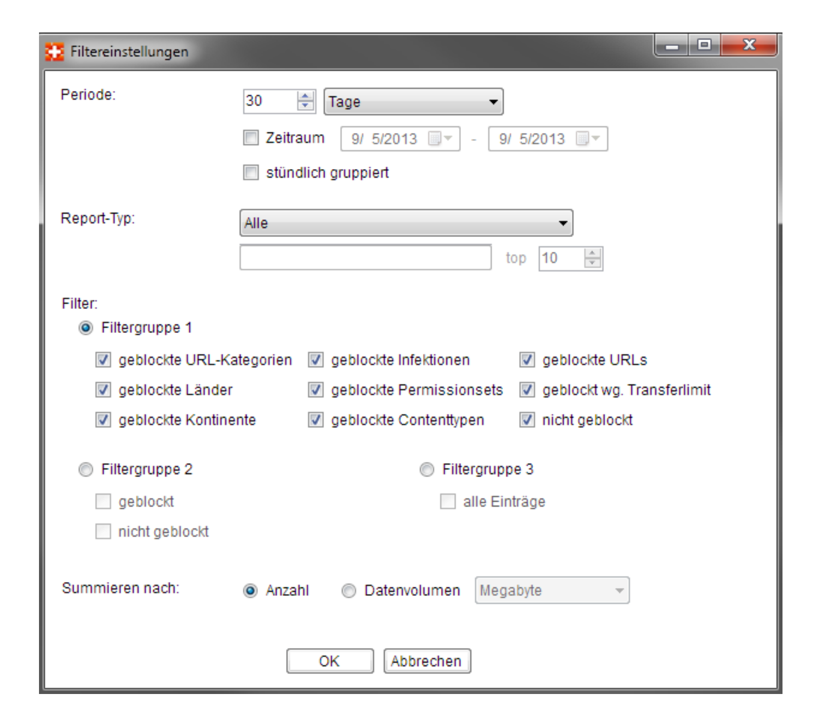


Abbildung 43: Reporting: Filtereinstellungen Web



Wert	Beschreibung
Periode/Zeitraum	Gibt an, über welchen Zeitraum ausgewertet werden soll. Mit Eingabe der Zahl können die letzten angegeben Zeiteinheiten (Stunden, Tage, Wochen, Monate, Quartale oder Jahre) ausgewählt werden, alternativ dazu kann der Zeitraum und die entsprechende Zeiteinheit angegeben werden. Maximal sind 100 Zeiteinheiten möglich, mit Wochen sind Kalenderwochen gemeint. Zeiteinheiten starten mit der ersten Einheit (Monatserster oder ein Tag mit Mitternacht).
Stündlich gruppiert	Über den angegebenen Zeitraum wird stündlich gruppiert und summiert, als Ergebnis erhält man eine stündliche Auswertung (0-1 Uhr, 1-2 Uhr, usw.).
Gruppieren	Die Gruppierungsoptionen lassen sich in folgende Gruppen aufteilen: • Alle Datensätze auswählen. • Gruppieren nach Permissionset, Source IP, Domain, Top Level Domain (TLD), Netzwerkgruppe oder Subnetz mit entsprechendem Parameter. • Gruppieren nach Subnetzen in Netzwerkgruppen, Permissionsets, Source IPs, Domains oder TLDs mit der größten Anzahl an bzw. Datenmenge für Requests. Ausgewählt werden die höchsten „top“ Einträge. • Gruppieren nach speziellem Permissionset, Source IP, Netzwerkgruppe oder Subnetz (jeweils mit Parameter), wobei die häufigsten oder größten Datenvolumen verursachenden Domains oder TLDs für die Auswahl angezeigt werden. • Gruppieren nach Kunden pro Standort (Netzwerkgruppe oder Subnetz), wobei ein Kunde durch eine eindeutige Source IP pro Stunde definiert ist.
Filter	Mit Hilfe der Filtergruppen lassen sich die zur Auswertung ausgewählten Daten weiter einschränken. In jeder Filtergruppe umfasst die Summe aller Flags immer 100%.
Filtergruppe 1	Hier kann nach unterschiedlichen Blockgründen ausgewählt und gefiltert werden.
Filtergruppe 2	Diese Gruppe bietet eine Zusammenfassung aller Blockgründe.
Filtergruppe 3	Es wird nicht gefiltert, alle Einträge werden zur Auswertung herangezogen.
Summiert nach	Es kann nach Anzahl der Einträge oder nach Datenvolumen in einer Einheit (Kilobyte, Megabyte oder Gigabyte) summiert werden.

Tabelle 37: Reporting: Filtereinstellungen Web



Filtereinstellungen für Typ Mail

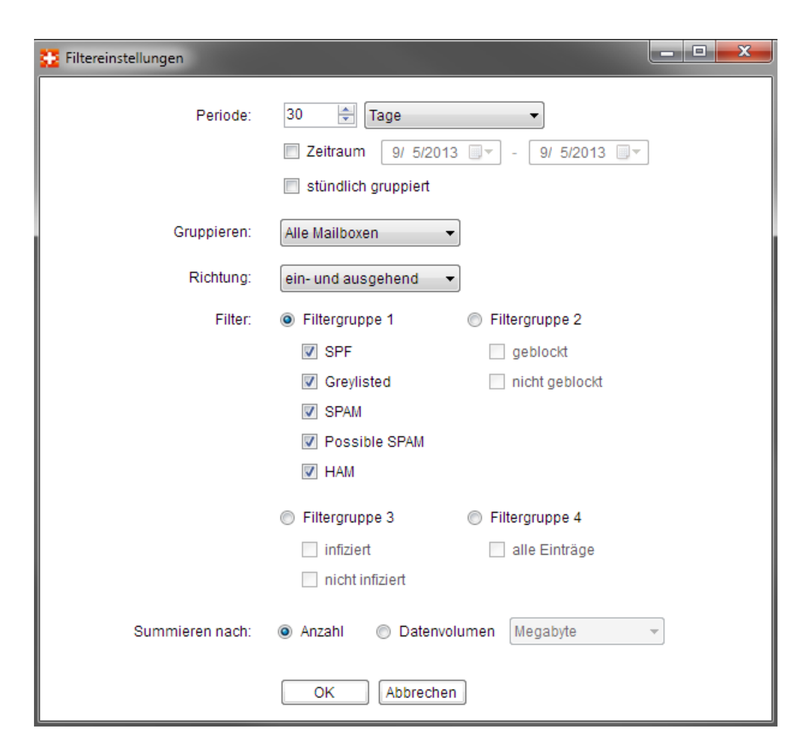


Abbildung 44: Reporting: Filtereinstellungen Mail



Wert	Beschreibung
Periode, Zeitraum, stündlich gruppiert, summiert nach	Analog zu Filtereinstellungen für Typ Web.
Gruppieren	Hier gibt es drei Optionen: • Alle Datensätze auswählen. • Gruppieren nach einer Mailbox mit Parameter. • Gruppieren nach Mailboxen mit den meisten oder größten Mails. Ausgewählt werden die höchsten „top“ Einträge.
Richtung	Gibt an, ob über eingehende, ausgehende oder beide Richtungen ausgewertet werden soll.
Filter	Mit Hilfe der Filtergruppen lassen sich die zur Auswertung ausgewählten Daten weiter einschränken. In jeder Filtergruppe umfasst die Summe aller Flags immer 100%.
Filtergruppe 1	Hier kann nach Bewertung des Mails gefiltert werden, d.h. Blocken aufgrund von SPF oder Greylisting bzw. die Spambewertung.
Filtergruppe 2	Mit Hilfe dieser Gruppe können geblockte und nicht geblockte Mails unterschieden werden. Hier können auch Spammails unter die geblockte Kategorie fallen, wenn die Spameinstellung ein Verwerfen oder Umleiten vorsieht.
Filtergruppe 3	Hier können Mails mit infizierten Anhängen sauberen Mails gegenübergestellt werden.
Filtergruppe 4	Es wird nicht gefiltert, alle Einträge werden zur Auswertung herangezogen.

Tabelle 38: Reporting: Filtereinstellungen Mail

3.15 Logdateien

Über den Menüpunkt Logdateien können Sie die aktuellen Logfiles von **IKARUS gateway.security** betrachten. Folgende Logs können hier angezeigt werden:

- **Global:** Inhalt des Files `splogfile.log`
- **Web:** Inhalt des Files `proxy.log`
- **E-Mail:** Inhalt des Files `mail.log`
- **Update:** Inhalt des Files `update.log`

Abbildung 45: Logdateien

3.16 Konfigurationsdatei

Hier können Sie die Konfigurationsdatei `securityproxy.conf` betrachten und editieren. Alle Konfigurationsparameter, die über das **IKARUS gateway.security Configuration Center** einstellbar sind, können manuell erfasst und editiert werden.

Sie sollten nur Änderungen an der Konfigurationsdatei vornehmen, wenn Sie sich absolut sicher sind, dass dies unumgänglich ist. In der Regel ist es aber nicht notwendig, die `securityproxy.conf` direkt zu editieren, da das **IKARUS gateway.security Configuration Center** sämtliche Optionen verwalten kann und es auch viel bequemer und sicherer ist.



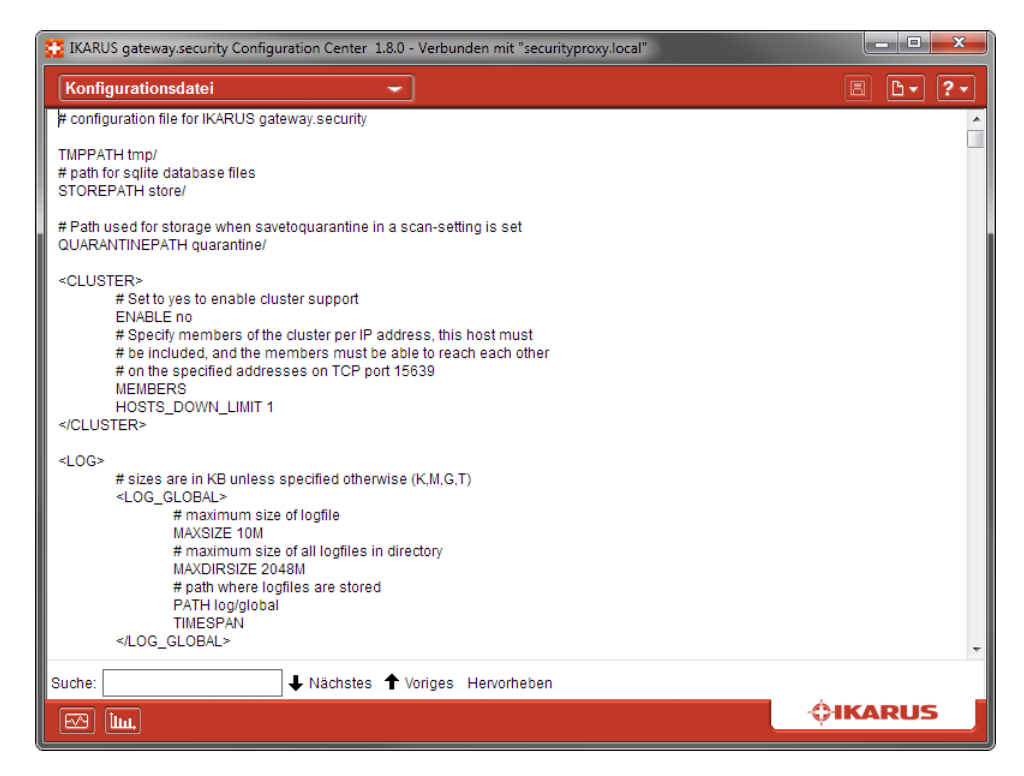


Abbildung 46: Konfigurationsdatei

3.17 Virusliste

Die Virusliste ist eine Aufstellung der von **IKARUS gateway.security** gefundenen Malware jeglicher Art, die über die verschiedenen möglichen Kanäle (z.B. HTTP, SMTP, POP3, usw.) gefiltert wurden. Mit einem Doppelklick auf einen Eintrag können Sie detaillierte Informationen über diese abrufen.

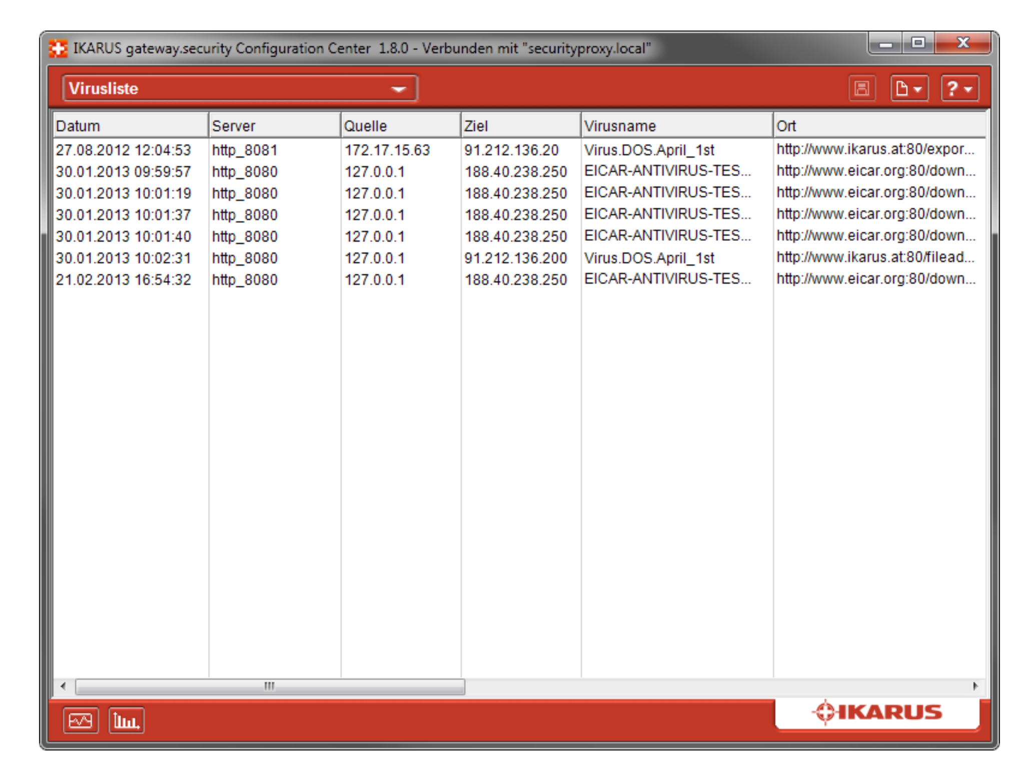


Abbildung 47: Virusliste

3.18 ActivityMonitor

IKARUS gateway.security bietet einen Überblick über die momentanen Aktivitäten seiner User. Mittels des ActivityMonitors kann das Mail- und Surfverhalten der User beobachtet werden.

Mittels des Buttons in der Fußzeile des **IKARUS gateway.security Configuration Centers** kann der ActivityMonitor aktiviert werden.

Dieser Dialog läuft neben dem **IKARUS gateway.security Configuration Center** – wird aber mitbeendet.



Abbildung 48: ActivityMonitor

Aktivierte Protokolle können hier beobachtet werden. Deaktivierte Protokolle werden ausgegraut.

Skalierung der X- als auch der Y-Achse sind möglich, es kann aber auch die Auto-Skalierung verwendet werden.

3.19 Anzeige der Reports

Um die in der Konfigurationsdatei definierten Reports anzeigen zu können, gibt es ein eigenes Dialogfenster.

Dieses kann auf zwei Arten geöffnet werden:



1. Mittels Reporting-Button in der Fußzeile des **IKARUS gateway.security Configuration Centers**: 
2. Mittels Reporting-Button im Login-Dialog. Hierbei ist zu beachten, dass auch hier gültige Logininformationen zu verwenden sind.

Beide Varianten öffnen den folgenden Dialog, in welchem die Reports angezeigt werden:

Abbildung 49: Anzeige der Reports

Wert	Beschreibung
Button „Report anzeigen“	Der in der ComboBox gewählte Report wird erstellt und im Feld darunter angezeigt.
Button „Drucken“	Öffnet einen Druck-Dialog, mit dessen Hilfe der gezeigte Report ausgedruckt werden kann.
Button „Schließen“	Schließt den Anzeigedialog des Reportings.

Tabelle 39: Anzeige der Reports



4 Verwendung von IKARUS gateway.security

4.1 IKARUS gateway.security als MX Gateway

4.1.1 Überblick

IKARUS gateway.security kann als Mail Exchange Gateway (MX) eingesetzt werden und erlaubt so den Viren- und SPAM-freien Empfang von eingehenden E-Mails. Diese Konfiguration setzt voraus, dass sie für Ihre Domäne einen eigenen DNS Server zur Verfügung haben, um den entsprechenden MX Eintrag zu setzen. Darüber hinaus wird davon ausgegangen, dass in Ihrem internen Unternehmensnetz ein eigener Mailserver steht.

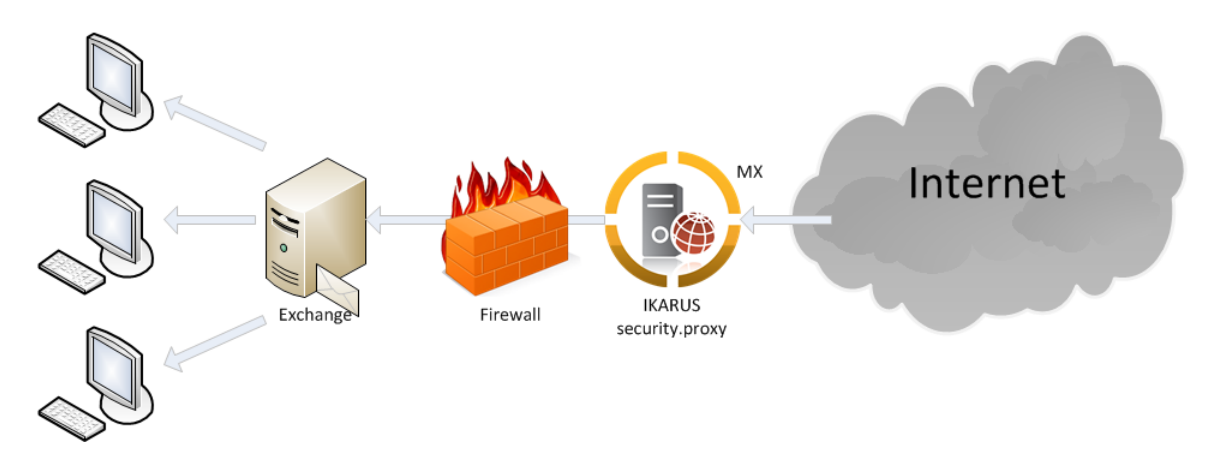


Abbildung 50: Überlick MX-Gateway

4.1.2 Voraussetzungen

Der MX Eintrag für ihre Domäne muss entsprechend gesetzt sein und auf die extern erreichbare IP-Adresse von **IKARUS gateway.security** zeigen. Bitte beachten Sie bei der Konfiguration ihrer Firewall, dass **IKARUS gateway.security** vom Internet aus erreichbar sein muss.

4.1.3 Einstellungen in IKARUS gateway.security

Es wird davon ausgegangen, dass das SMTP-Service von **IKARUS gateway.security** deaktiviert ist.

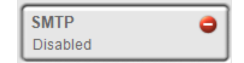
1. Damit **IKARUS gateway.security** als MX Gateway eingesetzt werden kann, muss die IP-Adresse, welche über das Internet erreichbar ist, gebunden werden. Sie erfassen hierzu entweder die entsprechende IP-Adresse der Netzwerkkarte, oder, wenn **IKARUS gateway.security** an allen verfügbaren Netzwerk Interfaces lauschen soll, die IP-Adresse `0.0.0.0` (Standardeinstellung). Bitte beachten sie, dass für den Betrieb eines MX Gateways unbedingt der SMTP Standardport 25 verwendet werden muss.
2. Der nächste Schritt ist die Definition der Routen für eingehende Mails. Dabei legen sie fest, wie mit eingehenden Mails verfahren werden soll. Wenn ihr interner Mailserver beispielsweise exchange.example.com heißt und die zu betreuende Domäne `@example.com` ist, so erfassen sie die folgenden Werte:
   (a) Typ: Ziel-Domain/E-Mail. Im dazugehörigem Textfeld wird die Ziel-Domäne `example.com` erfasst



   (b) Auswahl der entsprechenden Scanregel, die angewandt werden soll
   (c) Richtung: inbound
   (d) Auswahl ob Greylisting oder SPF1 angewandt werden sollen
   (e) Aktion: Host auswählen und den Computernamen oder die IP-Adresse des Zielservers angeben (dieser muss ein SMTP-Server sein und auf Port 25 gebunden sein)

3. Fügen Sie die eben angelegte Routeneinstellung durch einen Klick auf hinzufügen der Liste der Routen hinzu. Im Bedarfsfall können Sie noch die Priorität der erfassten Routen ändern.

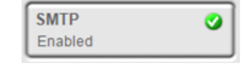
4. Wählen Sie im Übersichtsbaum den Punkt SMTP aus. Durch ein rotes Symbol wird signalisiert, dass das SMTP-Service derzeit deaktiviert ist.



5. Klicken Sie auf den SMTP-Button – nun ist ein gelbes Symbol sichtbar, was den bevorstehenden Statuswechsel des Services anzeigt.



6. Klicken Sie nun auf den Speichern Button . **IKARUS gateway.security** aktiviert nun das SMTP-Service mit den gewählten Einstellungen. Die erfolgreiche Aktivierung von SMTP wird durch ein grünes Symbol angezeigt.



4.2 IKARUS gateway.security als Mail-Relay

4.2.1 Überblick

IKARUS gateway.security ist auch in der Lage, als Mail-Relay für ausgehende E-Mails zu fungieren. Somit ist gewährleistet, dass auch ausgehende E-Mails auf Spam und Malware überprüft werden.

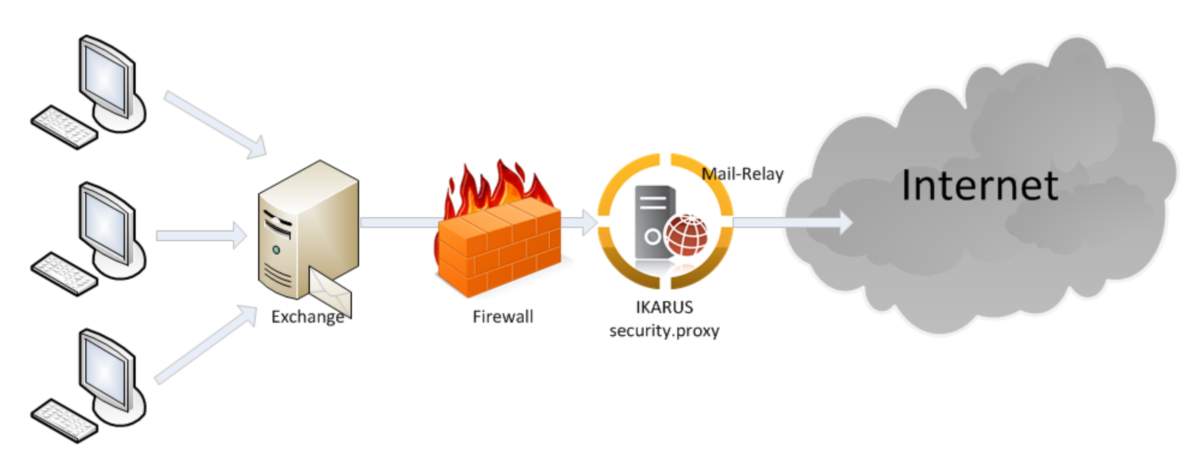


Abbildung 51: Überlick Mail-Relay



4.2.2 Voraussetzungen

Die Einstellungen an der unternehmensinternen Firewall müssen dementsprechend gesetzt sein, sodass **IKARUS gateway.security** von jenen Rechnern, die Mails versenden dürfen, erreicht werden kann. Es können noch Änderungen in der Konfiguration Ihres internen Mailservers vonnöten sein, um das Relaying von ausgehenden Mails über **IKARUS gateway.security** zu ermöglichen. Konsultieren Sie hierfür die Betriebsanleitung Ihres Mailservers.

4.2.3 Einstellungen in IKARUS gateway.security

Es wird davon ausgegangen, dass das SMTP-Service von **IKARUS gateway.security** deaktiviert ist.

1. Damit **IKARUS gateway.security** als Mail Relay eingesetzt werden kann, muss die IP-Adresse, über welche das Service erreicht werden soll, gebunden werden. Sie erfassen hierzu entweder die entsprechende IP-Adresse der Netzwerkkarte, oder, wenn **IKARUS gateway.security** an allen verfügbaren Netzwerk Interfaces lauschen soll, die IP-Adresse `0.0.0.0` (Standardeinstellung) – sollten sie **IKARUS gateway.security** nur als ausgehendes Relay verwenden, ist von einem Binding von `0.0.0.0` aus Sicherheitsgründen abzusehen.
2. Der nächste Schritt ist die Definition der Routen für ausgehende Mails. Dabei legen sie fest, wie mit ausgehenden Mails verfahren werden soll. Wenn ihr interner Mailserver beispielsweise die IP-Adresse `10.0.0.10` hat und sie nur E-Mails von diesen relayen wollen, müssen sie folgende Einstellungen in der Maske Einstellungen/Routen tätigen:
   (a) Typ: Client IP-Maske. Im dazugehörigem Textfeld wird die IP-Adresse des internen Mailservers `10.0.0.10/32` erfasst
   (b) Auswahl der entsprechenden Scanregel, die angewandt werden soll
   (c) Richtung: outbound
   (d) Aktion: Mails, die ins Internet relayed werden, müssen die Aktion MX verwenden, damit **IKARUS gateway.security** diese an den richtigen Zielserver weiterleiten kann
3. Fügen Sie die eben angelegte Routeneinstellung durch einen Klick auf hinzufügen der Liste der Routen hinzu. Im Bedarfsfall können Sie noch die Priorität der erfassten Routen ändern.
4. Wählen sie im Übersichtsbaum den Punkt SMTP aus. Durch ein rotes ‚Lämpchen' (Indikator) wird signalisiert, dass das SMTP Service derzeit deaktiviert ist.



5. Klicken sie auf den SMTP-Button – der Indikator ändert die Farbe auf Gelb, was den bevorstehenden Statuswechsel des Services anzeigt.



6. Klicken sie nun auf den Speichern Button . **IKARUS gateway.security** aktiviert nun das SMTP Service mit den gewählten Einstellungen. Die erfolgreiche Aktivierung von SMTP wird durch den grünen Indikator angezeigt.





Wenn mehrere Rechner im internen Netz Mails über **IKARUS gateway.security** verschicken sollen, so tragen sie diese entweder einzeln ein oder, falls ein ganzes Subnetz betroffen ist, die Netzadresse inklusive der Subnetzmaske (also z.B. `192.168.0.0/24`).

4.3 Greylisting

Greylisting bezeichnet eine Methode zur Erkennung von Mailservern (MTA = Mail Transfer Agent), über die Spam versendet wird. E-Mails werden nur weitergeleitet, wenn sie die *Greylisting*-Überprüfung bestehen.

Bei dieser Überprüfung wird davon ausgegangen, das vertauenswürdige MTAs ensprechend RFC821 implementiert sind und versuchen, temporär abgelehnte E-Mails innerhalb eines bestimmten Zeitraums erneut zu vesenden.

IKARUS gateway.security (SP) unterstützt *Greylisting* mit optionalem temporärem Whitelisting. Wird ein MTA nach erfolgter *Greylisting*-Überprüfung als vertrauenswürdig eingestuft, kann er temporär in eine Whitelist eingetragen werden.

Ist die IP-Adresse eines sendenden MTA nicht in der permanenten Whitelist enthalten, so wird die Verbindung der *Greylisting*-Überprüfung unterzogen.

Ist temporäres Whitelisting aktiviert, so wird die IP des Senders in eine Whitelist eingetragen. Somit wird für eine bestimmte, zu konfigurierende Zeitspanne, jede E-Mail von dieser IP-Adresse weitergeleitet.

Anmerkung: Temporäres Whitelisting ist aktiviert, sobald für die Dauer ein Wert ungleich Null eingetragen ist (siehe 3.10.2).

Nach Ablauf dieser Zeitspanne wird ein erneuter Verbindungsversuch wieder dem *Greylisting* unterzogen. Danach kann die Adresse, abhängig vom Ergebnis der Überprüfung, erneut in die temporäre Whitelist eingetragen werden.

4.4 Der URL-Filter

Der **IKARUS gateway.security** URL-Filter bietet Ihnen die Möglichkeit Themenbereichsweise oder Standortweise das Internet zu „verwalten“.

4.4.1 Wie konfiguriere ich den URL-Filter?

Der URL-Filter umfasst derzeit drei große Bereiche:

- URL-Kategorien
- Länderfilter
- Kontinentfilter

Die Konfiguration ist für alle drei Bereiche gleich:



- Öffnen Sie ein Permission-Set.
- Wählen Sie im Drop-down-Menü Typ

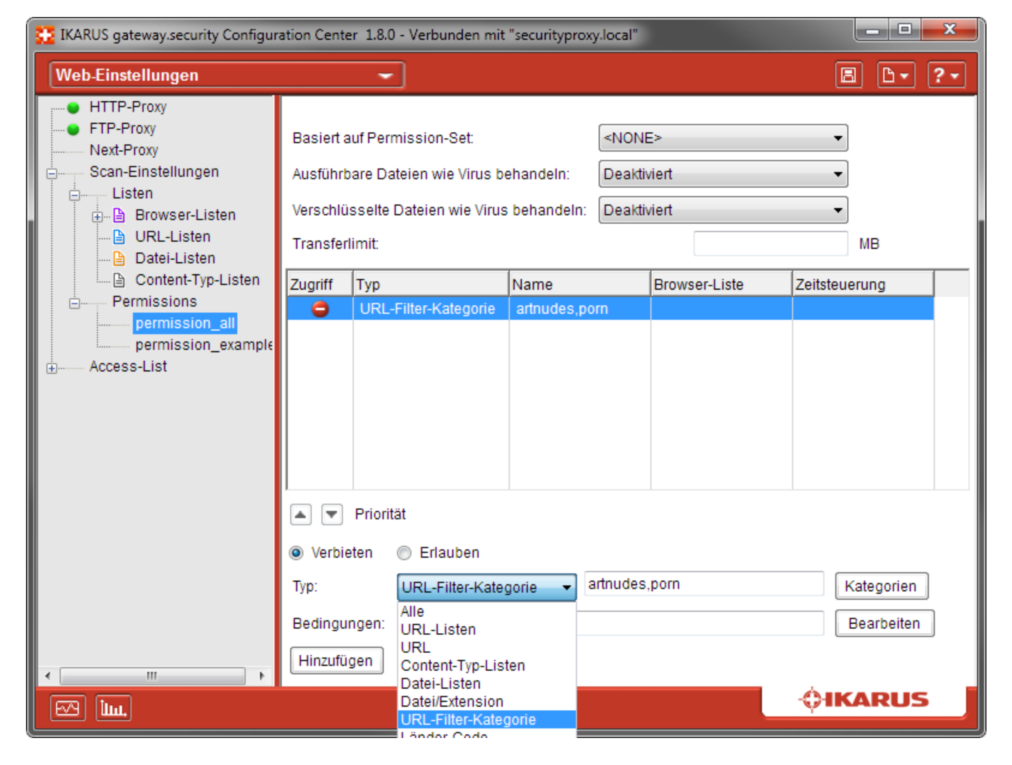


Abbildung 52: URL-Filter

- Klicken Sie auf die Schaltfläche rechts am Ende der Zeile.



- Wählen Sie die gewünschten Kategorien bzw. Länder oder Kontinente aus der Liste und markieren diese mit einem Hakerl, dann klicken Sie auf OK. Beispiel URL-Filter-Kategorien:

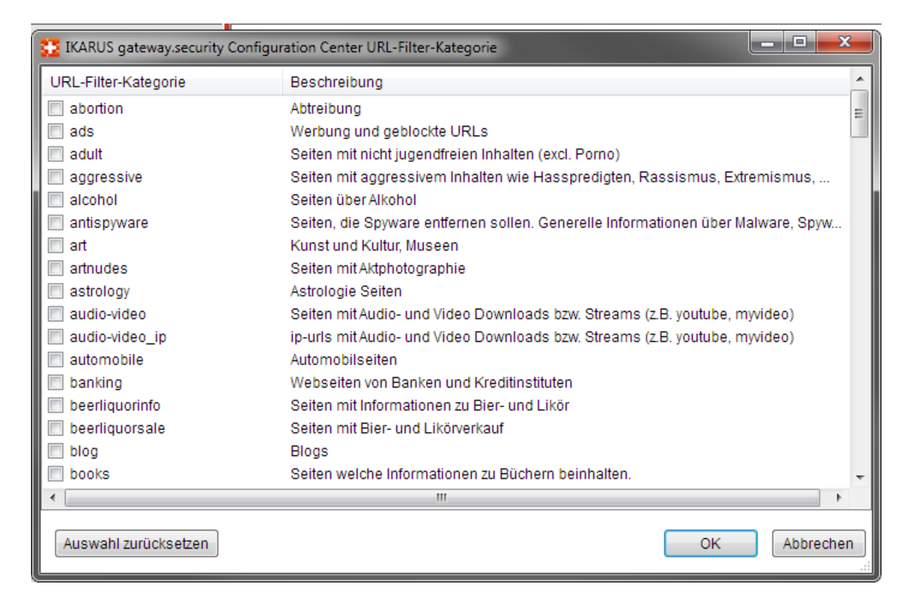


Abbildung 53: URL-Filter-Kategorien



- Nun fügen Sie die Permission hinzu.

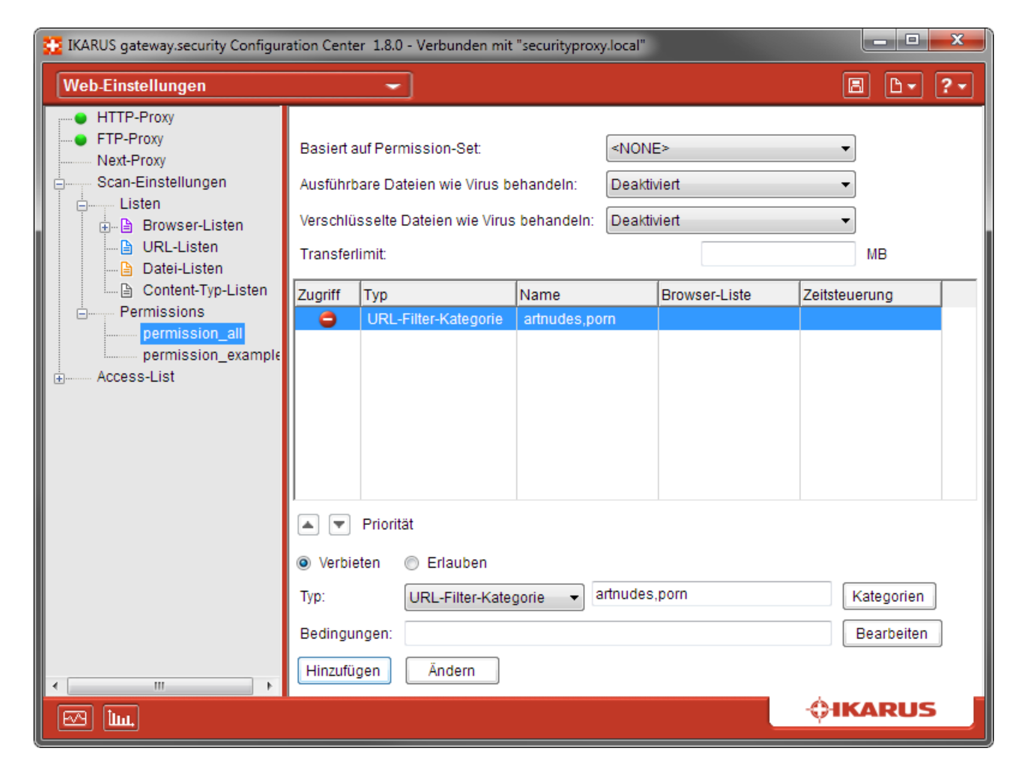


Abbildung 54: Permission

Beispiel:

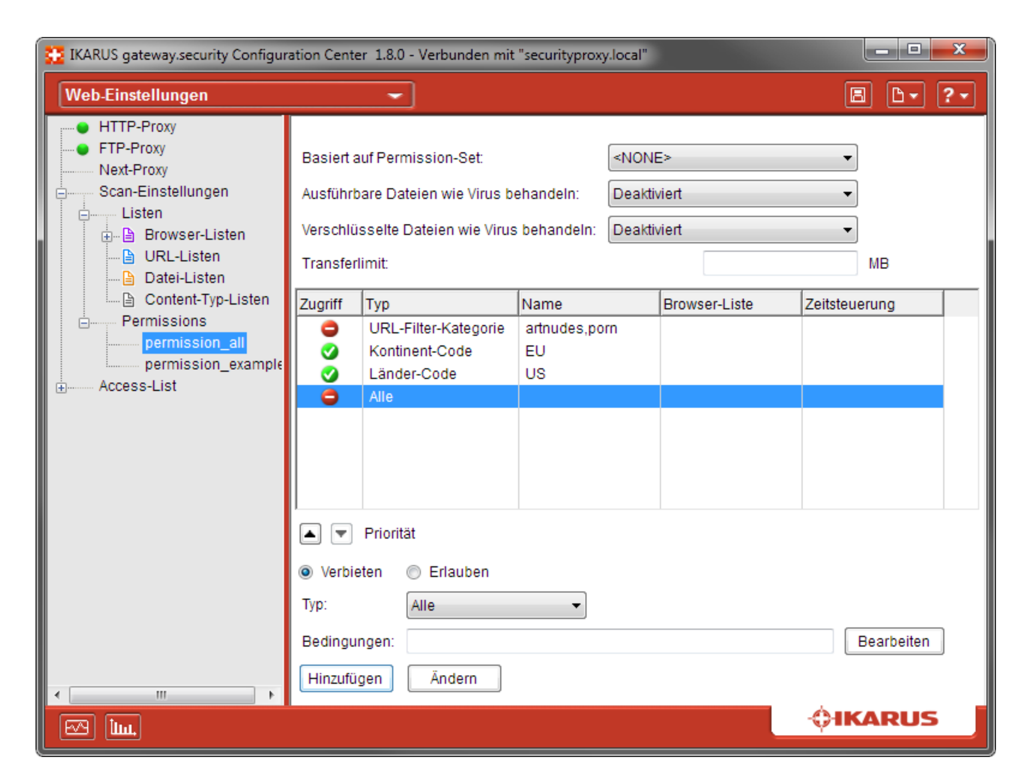


Abbildung 55: Permission-Sets

Dieses Permission-Set bewirkt folgendes:

- Alle URLs der Kategorien „artnudes“ und „porn“ werden geblockt.
- Alle URLs aus der EU (außer die oben genannten Kategorien) werden erlaubt.
- Ebenso alle URLs aus den „United States“.
- Alle anderen Zugriffe werden geblockt.

Alle Zugriffe, außer URLs aus US oder EU die nicht „artnude“ oder „porn“ kategorisiert wurden, werden geblockt.

4.4.2 Branding

IKARUS gateway.security zeigt dem Benutzer verschiedene Webseiten an, wenn er sich für den Internetzugang anmeldet, oder der Zugriff auf eine bestimmte Seite geblockt wird.

Diese Webseiten können für verschiedene Netzwerk-Anbieter (d.h. verschiedene Routen) unterschiedlich gestaltet werden. Die Gesamtheit dieser für den Anbieter spezifischen Gestaltung wird als *Branding* bezeichnet.

Die HTML-Vorlagen für die verschiedenen Brandings werden in gleichnamigen Unterverzeichnissen des `conf` Verzeichnisses abgelegt.

```
conf/
    messages/
        filiale1/
            lockpage.html
        filiale2/
            lockpage.html

    ...
```

Der Zugriff auf die in diesen Templates referenzierten Ressourcen (CSS, Images, etc.) muss durch entsprechende Konfiguration der Web-Server sichergestellt werden.

Über die Zuordnung eines Brandings in der Access-List (siehe 3.9.5) wird festgelegt, welches Branding für bestimmte IP-Adressen bzw. Subnetze zu verwenden ist.

4.5 E-Mails via Transport Layer Security

4.5.1 Überblick

IKARUS gateway.security ist in der Lage E-Mails unter Benutzung von Transport Layer Security verschlüsselt zu versenden oder zu empfangen.

4.5.2 Voraussetzungen

Für die Aktivierung von TLS ist keine Config-Option vonnöten – alles was dafür benötigt wird, sind ein Key- und Certificatefile. Diese beiden Files können selbst erstellt sein (z.B. mit OpenSSL). Das Zertifikatsfile (Cer-

tificatefile) muss signiert sein – dies kann selbst oder von einem Zertifizierungsdienstanbieter signiert sein.

Für das Erstellen von selbst signierten Zertifikaten gibt es unzählige Tutorials im Internet – für den Produktiv-Betrieb empfiehlt es sich jedoch aus Sicherheitsgründen, sich das Zertifikat von einem professionellen Zertifizierungsdienstanbieter erstellen zu lassen.

Key- und Certfile müssen im Installationsverzeichnis von **IKARUS gateway.security** unter

```
/IKARUS/security.proxy/conf/certs
```

abgespeichert sein. Dabei ist der Name der Files irrelevant, solange das Zertifikatsfile auf die Dateiendung .crt und das Keyfile auf die Dateiendung .key endet.

Nach erfolgreicher Speicherung und Restart des SMTP-services ist **IKARUS gateway.security** bereit, das Versenden bzw. Empfangen von Mails via TLS durchzuführen.

- Der Mailversand über TLS erfolgt automatisch, wenn der Zielserver TLS unterstützt. Ansonsten erfolgt der Versand unverschlüsselt.
- Der Empfang von Mails via TLS ist abhängig davon, ob der sendende Server TLS unterstützt und die Übertragung der E-Mails mittels TLS initiiert.

4.5.3 Wie überprüfe ich, ob TLS aktiv ist?

Um zu überprüfen, ob Key und Certificate richtig eingespielt wurden, können Sie eine Verbindung zu **IKARUS gateway.security** mittels Telnet herstellen:

```
Client (C): telnet <servername> 25
Server (S): 220 <servername> \isp SMTP-Server ready
C: EHLO foo
S: 250-<servername>
    250 STARTTLS
C: QUIT
S: 221 closing connection
```

Achten Sie darauf, dass **IKARUS gateway.security** in der Antwort auf den EHLO-Befehl die Zeile 250 STARTTLS zurückgibt. Dies gibt an, dass der Server bereit für TLS Verbindungen ist. Falls OpenSSL auf ihrem System installiert ist, können Sie auch die Erstellung des TLS-Handshakes über die Kommandozeile mit folgendem Befehl überprüfen:

```
% openssl s_client -starttls smtp -crlf -connect <servername or IP-Address>:25
```

4.6 Konfiguration für LDAP-Authentifizierung

4.6.1 Überblick

Dieses Kapitel beschreibt die Konfiguration von **IKARUS gateway.security** in Verbindung mit einem LDAP Server (z.B. Windows Active Directory). Dies erlaubt die Authentifizierung von Domänenbenutzern bei der Benutzung des HTTP-Proxy.



Das Lightweight Directory Access Protocol (LDAP) ist ein Protokoll, welches die Abfrage und Modifikation eines Verzeichnisdienstes über ein IP-Netzwerk erlaubt. Bekanntester Vertreter ist Microsofts Active Directory, welches in Serverprodukten wie Windows 2008 oder Windows Small Business Server zur Anwendung kommt.

Mithilfe von LDAP ist es möglich, im Active Directory angelegte Gruppen und Benutzer für die Authentifizierung **IKARUS gateway.security** zu verwenden. Dies erlaubt Ihnen z.B. aufgrund der Gruppenzugehörigkeit spezielle Permissionsets zu konfigurieren. Die Benutzer melden sich bei **IKARUS gateway.security** mit ihren Domänenbenutzer und Passwort an und erhalten gemäß ihrer Gruppenzugehörigkeit die entsprechenden Rechte zum ansurfen von Webseiten.

4.6.2 Voraussetzungen

Um **IKARUS gateway.security** mit LDAP zu benutzen, müssen folgende Voraussetzungen erfüllt werden:

- Ein konfigurierter LDAP-Server (z.B. ein Windows Domaincontroller), welcher von **IKARUS gateway.security** aus erreichbar ist, muss vorhanden sein.
- Ein Domänenbenutzer, welcher von **IKARUS gateway.security** zum Abfragen der LDAP-Daten verwendet wird, muss angegeben werden. (es kann prinzipiell jeder Domänenbenutzer verwendet werden, aus Sicherheitsgründen empfehlen wir aber, einen speziellen Benutzer für diese Abfragen anzulegen)

4.6.3 Einstellung des LDAP-Pfades

Um die Verbindung von **IKARUS gateway.security** zum LDAP-Server zu ermöglichen, müssen Sie den LDAP-Pfad erfassen. Sie finden diese Einstellung im Menü Global.

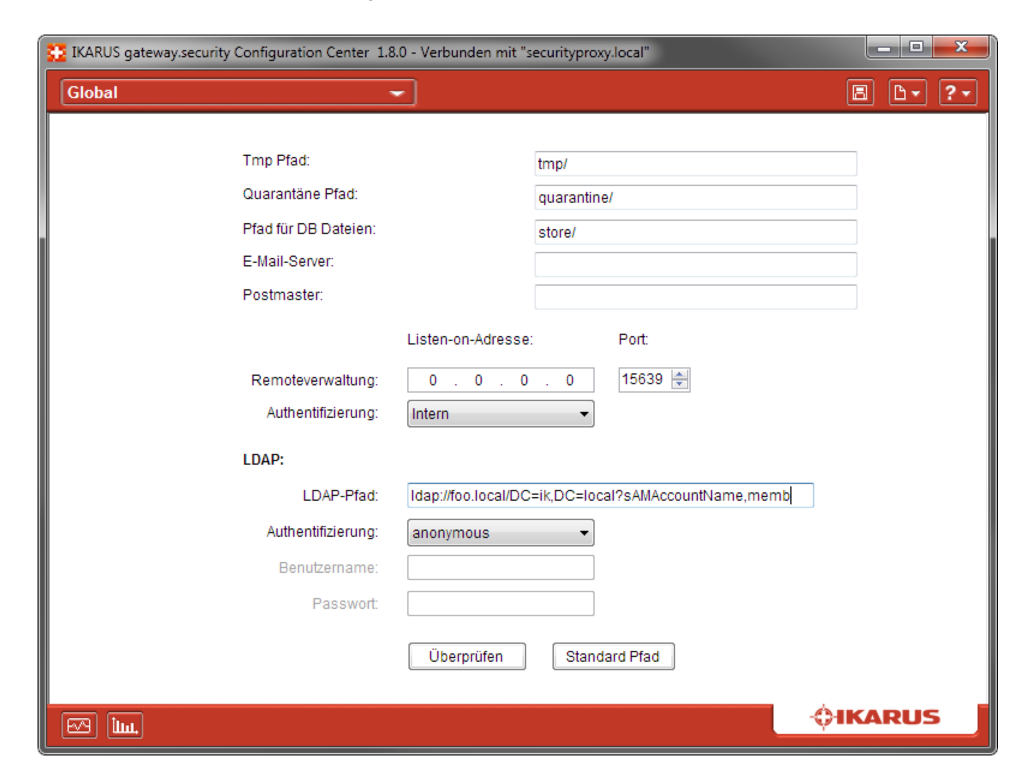


Abbildung 56: Definition LDAP-Pfad

Der LDAP-Pfad ist folgendermaßen aufgebaut:

```
ldap://foo.local/DC=ik,DC=local?sAMAccountName,memberOf?sub?(objectClass=person)
```

Anmerkung: Ersetzen sie foo.local mit ihrem tatsächlichen Domänennamen

Ein Tipp: Für die sichere Übertragung der LDAP-Daten empfehlen wir die Verwendung von ldaps. Hierzu ändern Sie einfach am Beginn des LDAP-strings das `ldap://` in `ldaps://`. Diese Option ist allerdings nur möglich, sofern ihr LDAP-Server dies unterstützt.

Konfigurieren Sie **IKARUS gateway.security** mit dem **IKARUS gateway.security Configuration Center**. Befindet sich der Server, auf dem der security.proxy installiert ist, innerhalb der Domäne, können Sie den korrekten LDAP-Pfad durch Drücken des Buttons ‚Standard Pfad' erfassen.

Zur Authentifizierung am LDAP-Server bietet **IKARUS gateway.security** zwei Möglichkeiten an:

- Anonymous (sofern ihr LDAP-Server dies unterstützt)
- Simple (hier benötigen sie einen gültigen Domänenbenutzer + Passwort)

Sie können vor dem Speichern die getroffenen Einstellungen durch Betätigen des Buttons ‚Überprüfen' auf ihre Richtigkeit überprüfen.

4.6.4 Anlegen von Permissionsets für LDAP-Gruppen

In den Web-Einstellungen können Sie nun Permissionsets für LDAP-Gruppen anlegen. Wir demonstrieren Ihnen das anhand eines Beispiels mit Microsoft Windows 2008.

Angenommen, Sie haben drei organisatorische Einheiten: Buchhaltung, Sales und Management. Alle drei Gruppen sind unter diesen Namen im Active Directory angelegt. Für jede dieser Gruppen wollen Sie nun ein spezielles Permissionset anlegen, welches die speziellen Surfberechtigungen der einzelnen organisatorischen Einheiten wiederspiegelt.

Legen Sie also für jede dieser Gruppen ein Permissionset an. Die Gruppennamen müssen ident mit den Gruppennamen im Active Directory sein. Damit **IKARUS gateway.security** diese Gruppen bei LDAP-Anfragen richtig zuordnet, müssen Sie diese Gruppen jedoch mit einem Präfix versehen. Es empfiehlt sich die Verwendung eines selbsterklärenden Präfix wie z.B. group_.

Sie legen also die Permissionsets gruppe_Buchhaltung, gruppe_Verkauf und gruppe_Verwaltung an. Ordnen Sie jeder dieser Gruppe die entsprechenden Berechtigungen (z.B. URL-Filter, Virenschutz, etc.) zu.

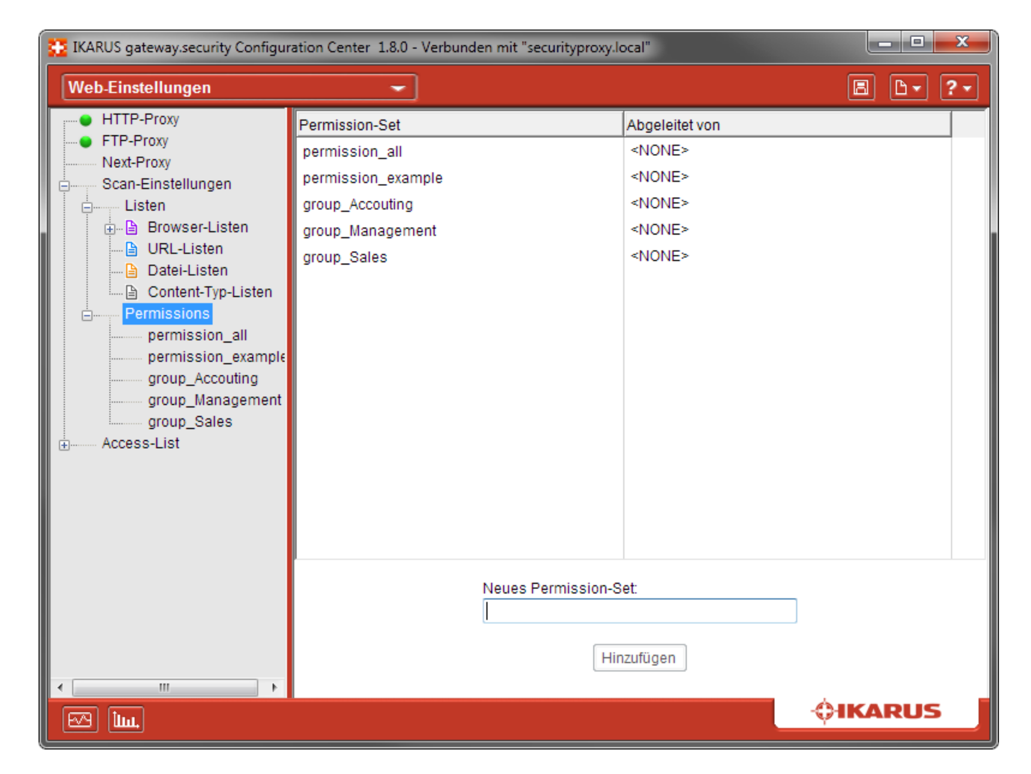


Abbildung 57: Permission-Sets LDAP

Speichern Sie die Änderungen.

4.6.5 Anlegen der Access-Lists für LDAP-Authentifizierung

Der letzte Schritt ist die Zuordnung von Access-Lists für die Benutzung von LDAP. Definieren Sie pro Accesslist die Netzwerkeinstellung und die Zugriffsberechtigungen und wählen Sie im Punkt ‚Authentifizierung' die Option LDAP Authentifizierung aus. Im Feld Permission-Set per Maske tragen Sie nun group_%g ein. Fügen Sie den eben erfassten Eintrag der Access-List durch Drücken auf den Button ‚Hinzufügen' hinzu.

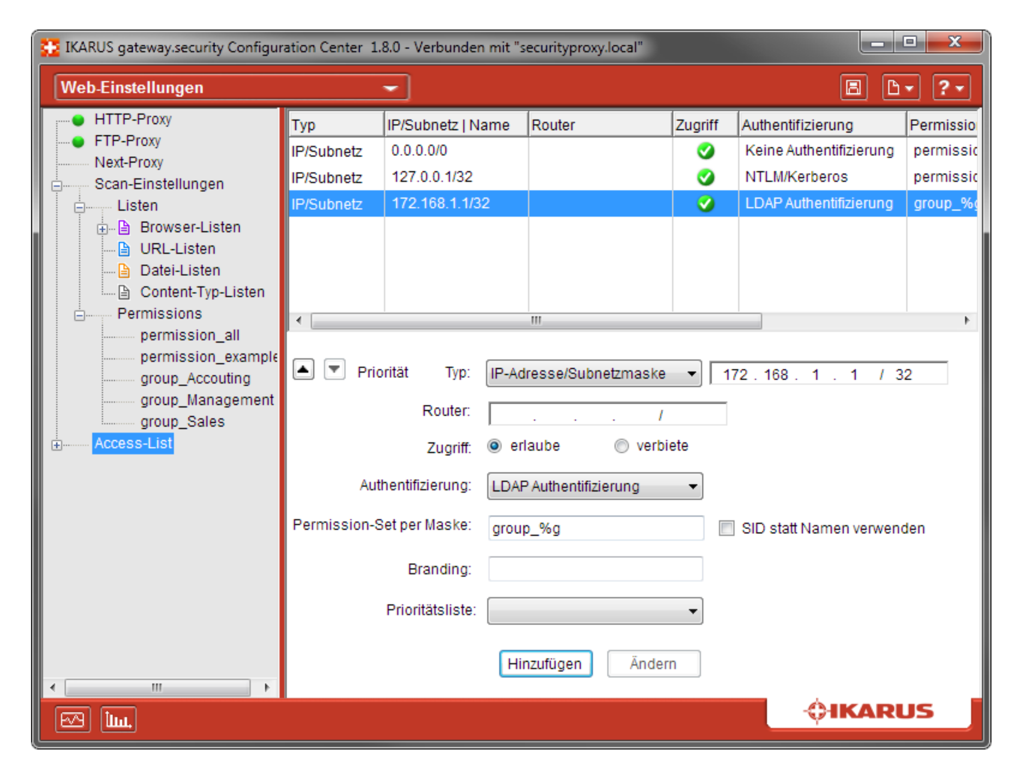


Abbildung 58: Access-List LDAP

Speichern Sie die Änderungen.

IKARUS gateway.security ist nun bereit für die Benutzung von LDAP.

4.6.6 Authentifizierung im Browser mittels LDAP

Ist der Browser Ihrer Wahl zur Benützung von **IKARUS gateway.security** konfiguriert, so erscheint beim ersten Aufruf einer Webseite ein Dialogfenster, das nach Benutzernamen und Passwort fragt. Der Benutzer erfasst hier seinen Benutzernamen und sein Passwort, welches er auch für die Anmeldung an der Windows-Domäne verwendet.

4.7 Authentifizierung über Startseite oder Formular

Die hier beschriebenen Authentifizierungsmethoden sind nur im Rahmen einer **wifi.security** oder **cloud.security**-Installation sinnvoll. In diesem Fall erfolgt der Zugriff vieler Endbenutzer mittels WLAN.

Den Benutzern wird entweder eine Startseite oder ein Formular angeboten, um sich für einen temporären Zugang zum Internet zu berechtigen. Die Dauer dieses Zugangs kann konfiguriert werden.

Startseite

Vom Betreiber des WLAN Netzes wird eine Seite erstellt, auf der z.B. Benutzer gebeten werden können, die AGB zu bestätigen, bevor Ihnen Zugang zum Netz gewährt wird. Über einen auf dieser Seite enthaltenen Link



wird die IP Adresse des Endgerätes freigeschalten.

Datensammlung

Die Benutzer werden beim ersten Zugriff auf das Netz auf eine Formularseite weitergeleitet. Dort muss zumindest eine E-Mail-Adresse eingegeben werden. Nach Abschicken des Formulars wird der Zugriff für einen kurzen Zeitraum (üblicherweise 5 Minuten) freigeschalten. Der Benutzer erhält in der Zwischenzeit eine E-Mail mit einem Link, über den er dauerhaften Zugang zum Netz erhält.

Wird dieser Link nicht betätigt, so wird nach den oben erwähnten 5 Minuten erneut das Formular zur Eingabe der Daten angezeigt. Nach einer konfigurierbaren Anzahl so fehlgeschlagener Authentifizierungsversuche wird der Zugang dauerhaft gesperrt. "Dauerhaft" bedeutet in diesem Zusammenhang: Für die Dauer der Verbindung, bis zum *session timeout*.

Welche Felder zusätzlich zur E-Mail-Adresse angegeben werden können oder müssen, kann der Betreiber konfigurieren.

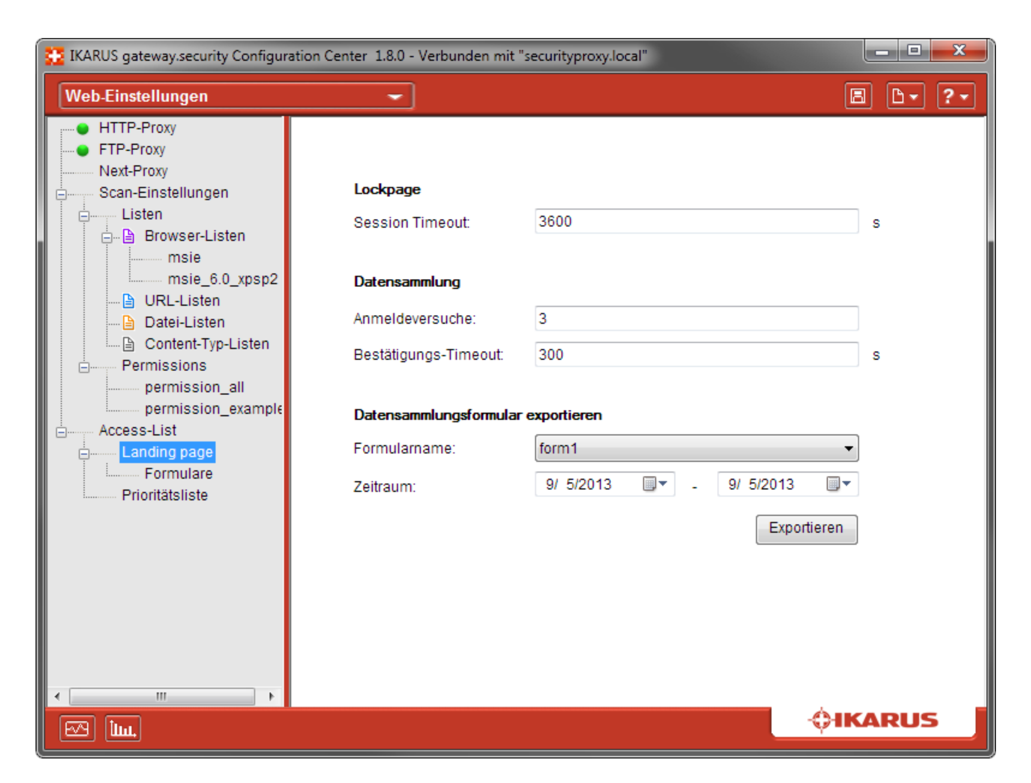


Abbildung 59: Allgemeine Konfiguration von Startseite und Datensammlung

Wert	Beschreibung
Session timeout	Zeitraum in [s], für den ein Zugang zum Internet gewährt wird. Nach Ablauf dieser Zeitspanne ist eine neuerliche Authentifizierung notwendig.
Anmeldeversuche	Anzahl der erlaubten Authentifizierungsversuche.
Bestätigungs-Timeout	Zeit in [s], die der Benutzer hat, um sich durch Betätigen des Bestätigungs-Links zu authentifizieren

Die von den Benutzern angegebenen Daten können zu einem späteren Zeitpunkt vom Betreiber abgefragt



werden.

Wert	Beschreibung
Formularname	Name des Formulars, für das die Eingaben abgefragt werden sollen.
Zeitraum	Es werden Dateneingaben aus dem angegebenen Zeitraum ausgegeben.
Exportieren	Die selektierten Daten als CSV Datei speichern.

Es können mehrere Formulare definiert werden.

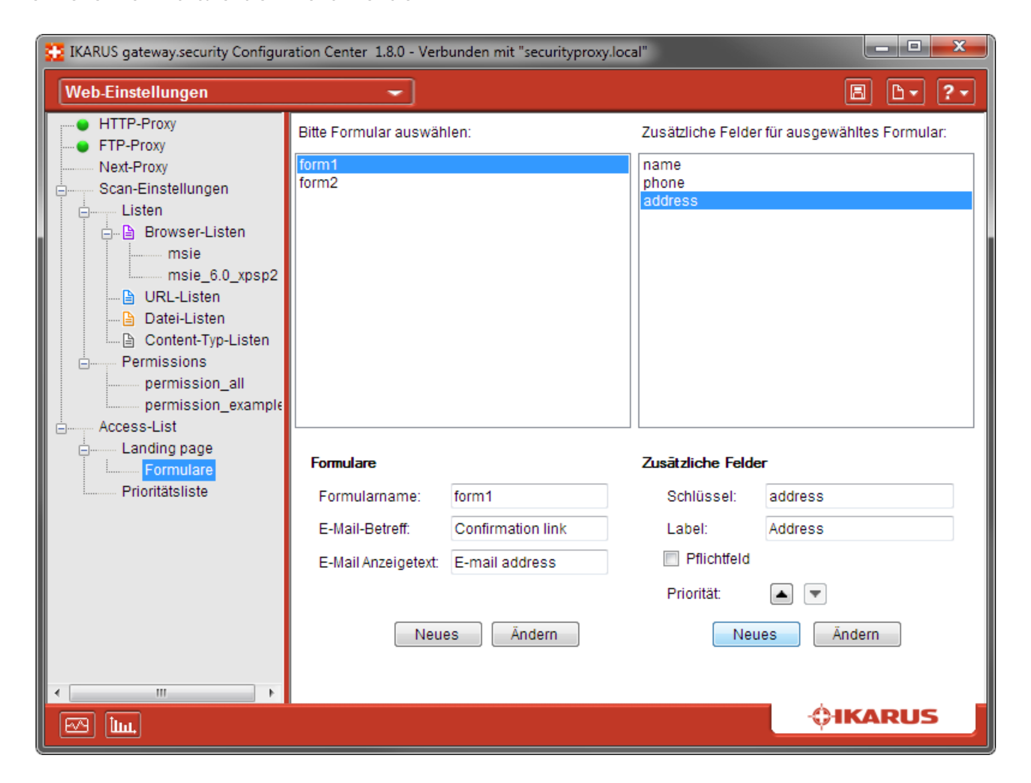


Abbildung 60: Konfiguration der Fomrulare

Wert	Beschreibung
Formularname	Eindeutige Bezeichnung des Formulars. Diese wird in den Netzwerk-Regeln referenziert, wenn die Authentifizierungsmethode "Datensammlungäusgewählt wird.
E-Mail-Betreff	Beteff-Zeile der E-Mail, die den Link zur Freischaltung des Zugangs enthält.
E-Mail-Anzeigetext	Beschriftung des Eingabefeldes für die E-Mail-Adresse im Formular

Zusätzlich zur E-Mail-Adresse können weitere Felder zum Formular hinzugefügt werden. Die Felder werden in der Reihenfolge der Liste im Formular angezeigt.

Wert	Beschreibung
Schlüssel	Eindeutiger Schlüssel für das Eingabefeld.
Label	Beschriftung des Eingabefeldes.
Pflichtfeld	Gibt an, ob das Feld vom Benutzer befüllt werden muss. Pflichtfelder werden im Formular **gelb** unterlegt.
Priorität	Verschiebt das ausgewählte Feld in der Liste nach oben oder unten.

4.8 Sicher surfen mit IKARUS gateway.security

IKARUS gateway.security kann als HTTP-Filter eingesetzt werden und erlaubt so das virenfreie Surfen durch das World Wide Web. Bitte beachten Sie, dass **IKARUS gateway.security** mit der Standardkonfiguration alle HTTP-Zugriffe zulässt.

4.8.1 Wie surfe ich über IKARUS gateway.security?

Um **IKARUS gateway.security** mit Standardkonfiguration zu verwenden, muss lediglich der HTTP-Dienst aktiviert (standardmäßig aktiviert) und im jeweiligen Browser der Proxy-Server eingestellt werden.

Um den HTTP-Dienst von **IKARUS gateway.security** zu aktivieren, klicken Sie einfach auf den Button und speichern Sie die Änderungen.

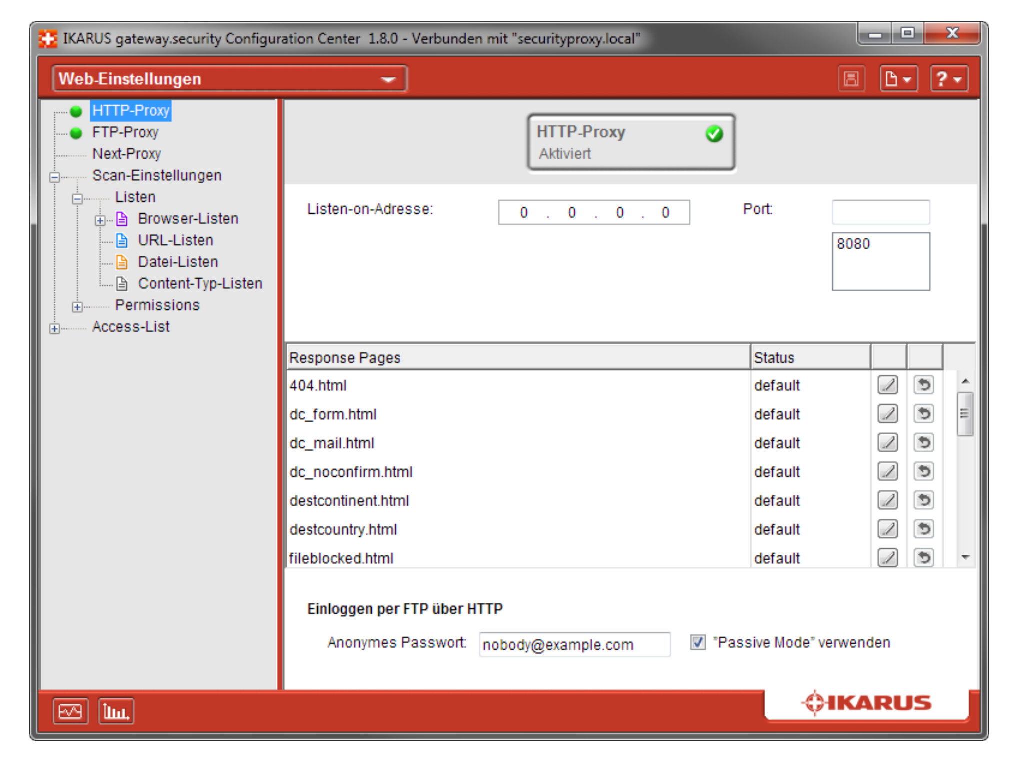


Abbildung 61: Einstellungen HTTP-Proxy





Sollten Sie nicht die Standardkonfiguration verwenden, stellen Sie sicher, dass ein Permission-Set angelegt wurde und dieses in der Access-List verwendet wird.

Permission-Set erstellen:

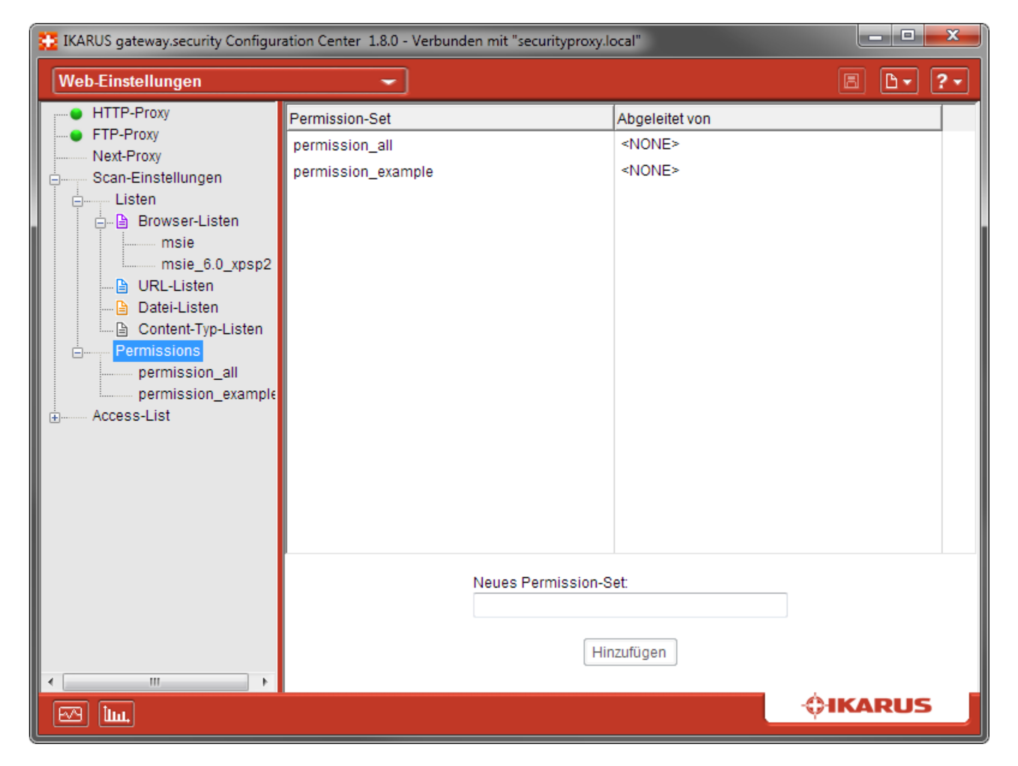


Abbildung 62: Erstellen von Permission-Sets

In der Access-List erfassen:

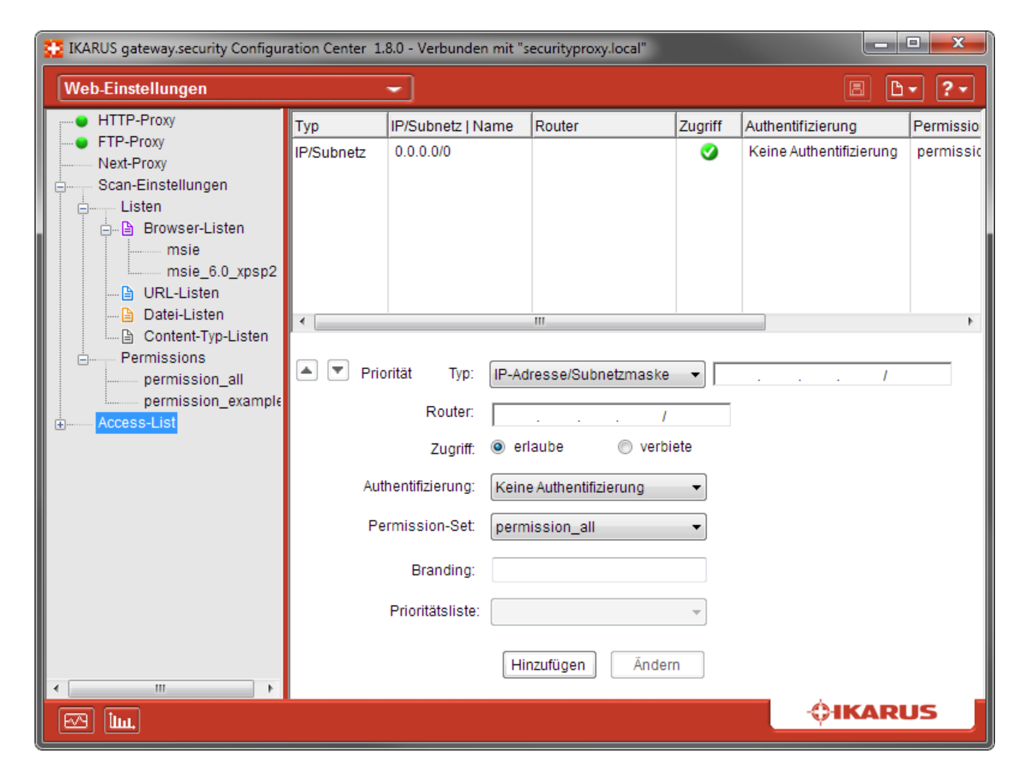


Abbildung 63: Konfigurieren von Access-Lists

4.8.2 Wie richte ich mein Permission-Set richtig ein?

Um URLs, Dateien, Content-Typen und Browser zu erlauben/blocken gehen Sie folgendermaßen vor:

1. Legen Sie eine Neue Liste des gewünschten Typs an

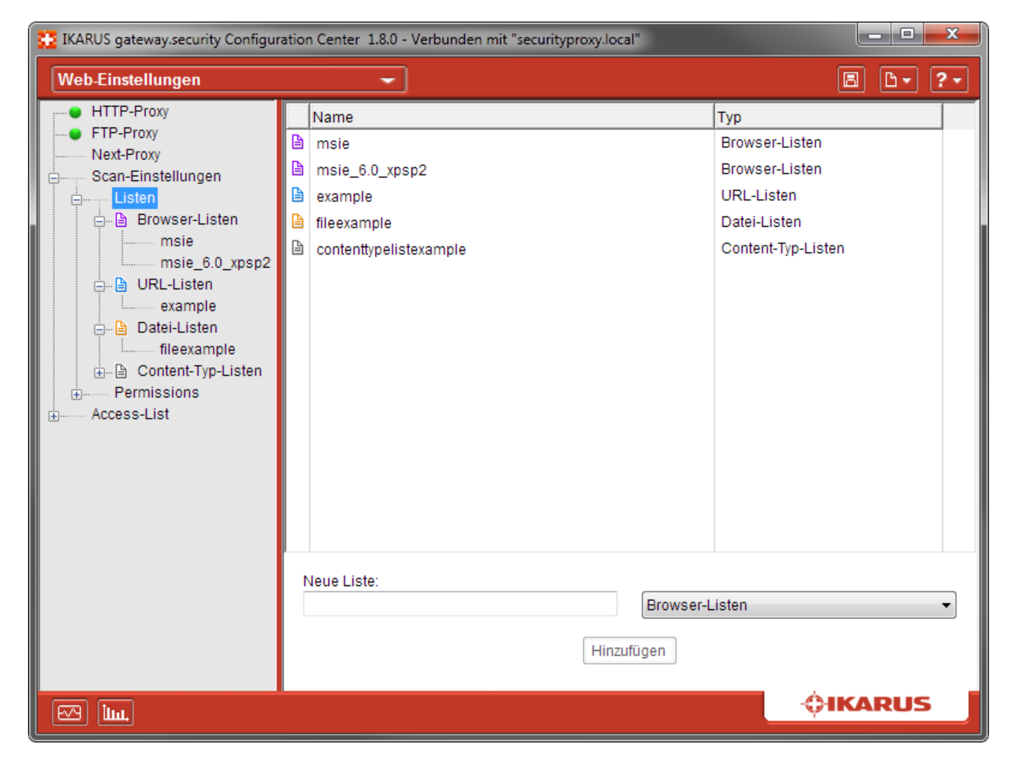


Abbildung 64: Einrichten Permission-Sets

2. Tragen Sie die Daten in der Liste ein (z.B. URLs)

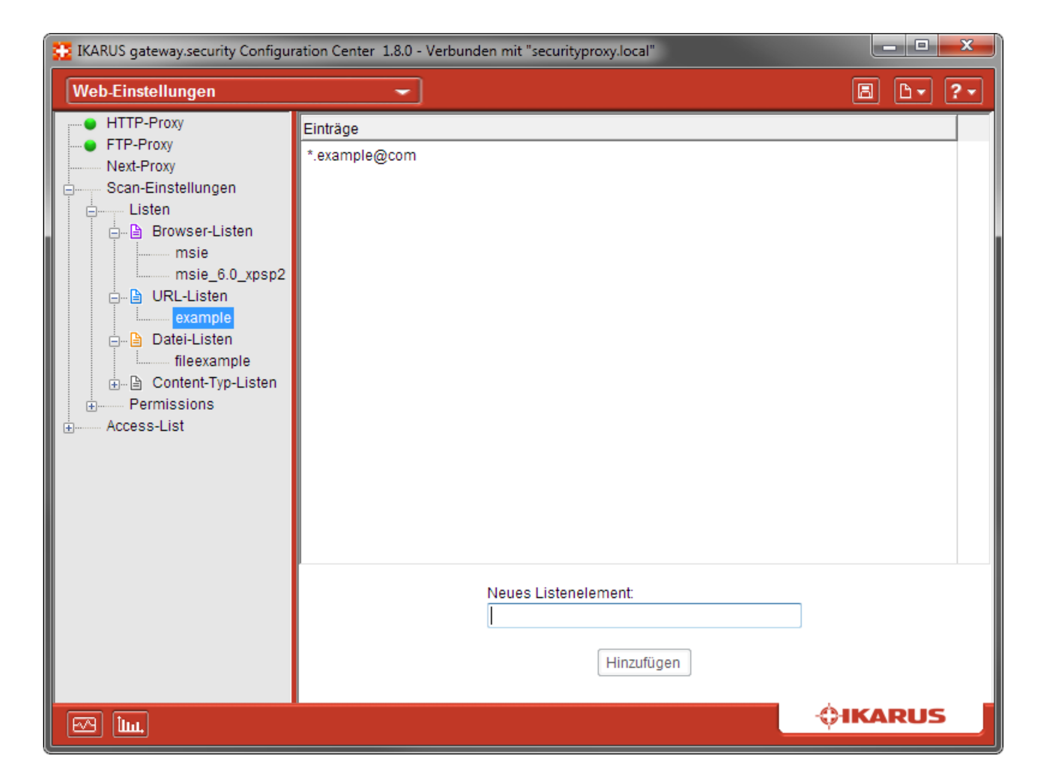


Abbildung 65: Einrichten URL-Listen

3. Erfassen Sie die Liste im Permission-Set

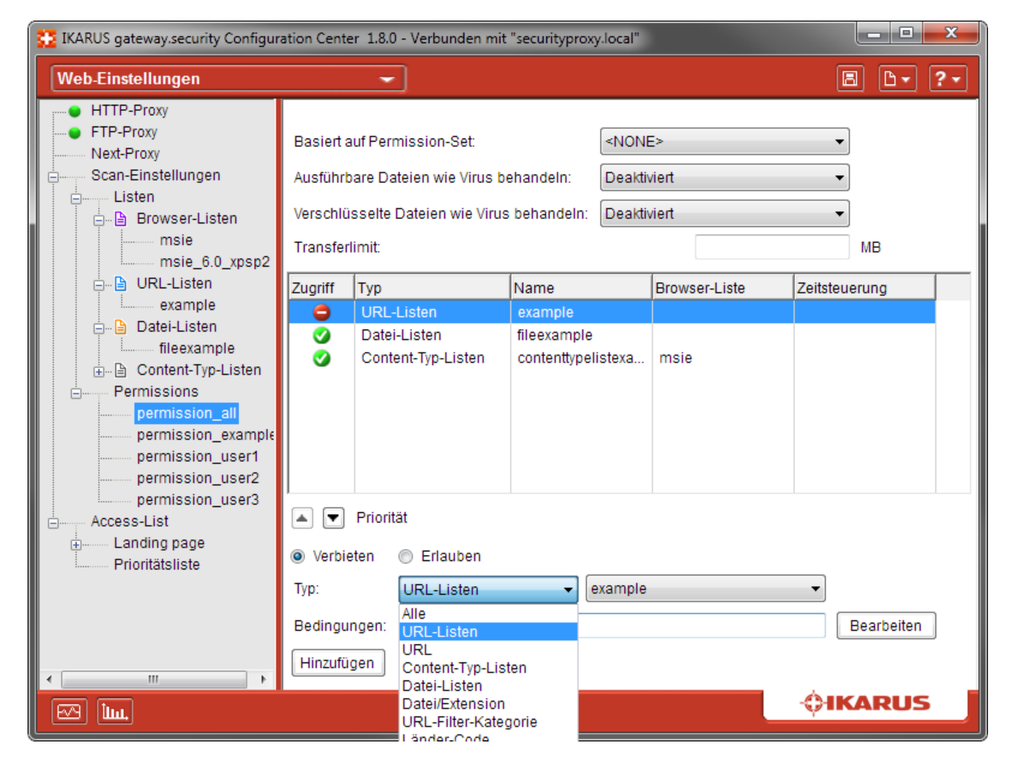


Abbildung 66: Erfassen URL-Liste im Permission-Set

4.8.3 Wie kann ich bestimmte Seiten / Domains / URLs blocken bzw. erlauben?

Um URLs bzw. Domains zu blocken ist zuallererst eine Erläuterung der Schreibweise erforderlich:

- Um eine Domain zu blocken:
  `www.example.com`
- Um eine Domain und alle ihre Subdomains zu blocken:
  `.example.com`
- Um nur die Subdomains zu blocken:
  `*.example.com`
- Um eine URL und alle Suburls zu blocken:
  `www.example.com/example`

Folgen Sie der Anleitung unter 4.8.2.

4.8.4 Wie kann ich Dateien blocken bzw. erlauben?

Folgen Sie der Anleitung unter 4.8.2.

4.8.5 Wie kann ich Content blocken bzw. erlauben?

Folgen Sie der Anleitung unter 4.8.2.



4.8.6 Was kann ich mit den Browser-Listen anfangen?

Diese Funktionalität erlaubt es Ihnen, den globalen Internetzugang (oder auch nur einzelne URLs) für gewisse Internet-Browser freizugeben oder zu sperren. Damit kann kontrolliert werden, welche Seiten mit welchem Internet Browser angesurft werden.

Zum Einsatz dieser Funktionalität

Sie legen wie in 4.8.2 beschrieben eine neue Liste an und tragen dort den User Agent String des jeweiligen Browsers ein.

So können Sie beispielsweise folgende Sicherheitseinstellung umsetzen:

- Internetzugriff auf beliebige Seiten darf nur mit einem alternativen Browser (z.B. Mozilla Firefox oder Opera) erfolgen.
- Der Microsoft Internet Explorer muss aber für die Microsoft Updates verwendet werden, daher kann dafür eine Ausnahmeregel eingesetzt werden.
- Einer der alternativen Browser hat z.B. Darstellungsprobleme mit der Online Banking Seite der Hausbank. Diese Seiten dürfen auch mit dem Internet Explorer besucht werden.
- Alle anderen URLs sind nur über die alternativen Browser erreichbar.

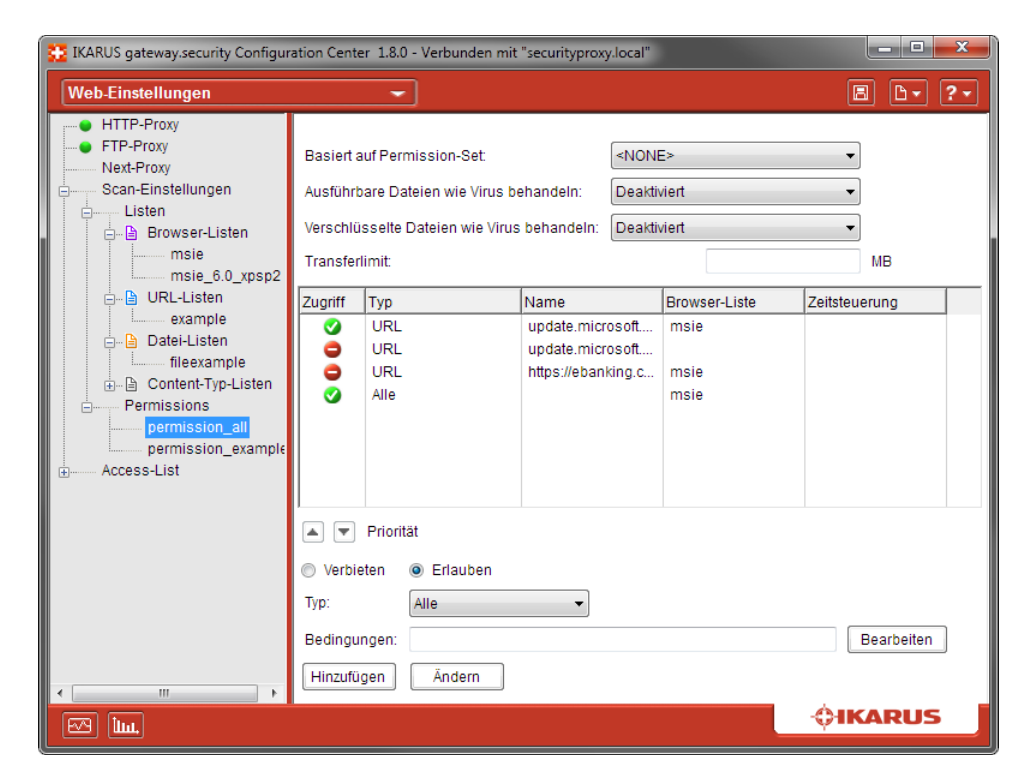


Abbildung 67: Einrichtung Browserlisten

4.8.7 Wie wende ich das Permission-Set richtig an?

Im Dialogfeld Access-List ordnen Sie dem Permission-Set eine IP-Adressen bzw. eine Netzwerkgruppe zu.



1. Wählen Sie bei Typ den IP-Bereich bzw. die Netzwerkgruppe
2. Selektieren Sie „Erlauben“
3. Wählen Sie die Art der Authentifizierung
   (a) Keine Authentifizierung (nicht per User/Passwort beschränkter Internetzugang)
   (b) Proxy-internal Authentifizierung (verwendet die **IKARUS gateway.security** Userverwaltung)
   (c) LDAP Authentifizierung (verwendet die Active Directory User und Gruppen)
   (d) Startseite. Der Benutzer ”authentifiziert” sich durch Klicken eines Links.
   (e) NTLM/Kerberos Authentifizierung (verwendet die Active Directory User und Gruppen)
   (f) Datensammlung.
4. Wählen Sie das Permission-Set, das verwendet werden soll bzw. geben Sie eine Maske für das Permission-Set ein.
5. Klicken Sie auf „Hinzufügen“

4.8.8 Wie verwende ich userspezifische Permission-Sets?

Sie haben also für mehrere User jeweils ein Permission-Set angelegt. Bsp.: Ihre User heißen „user1“, „user2“ und „user3“

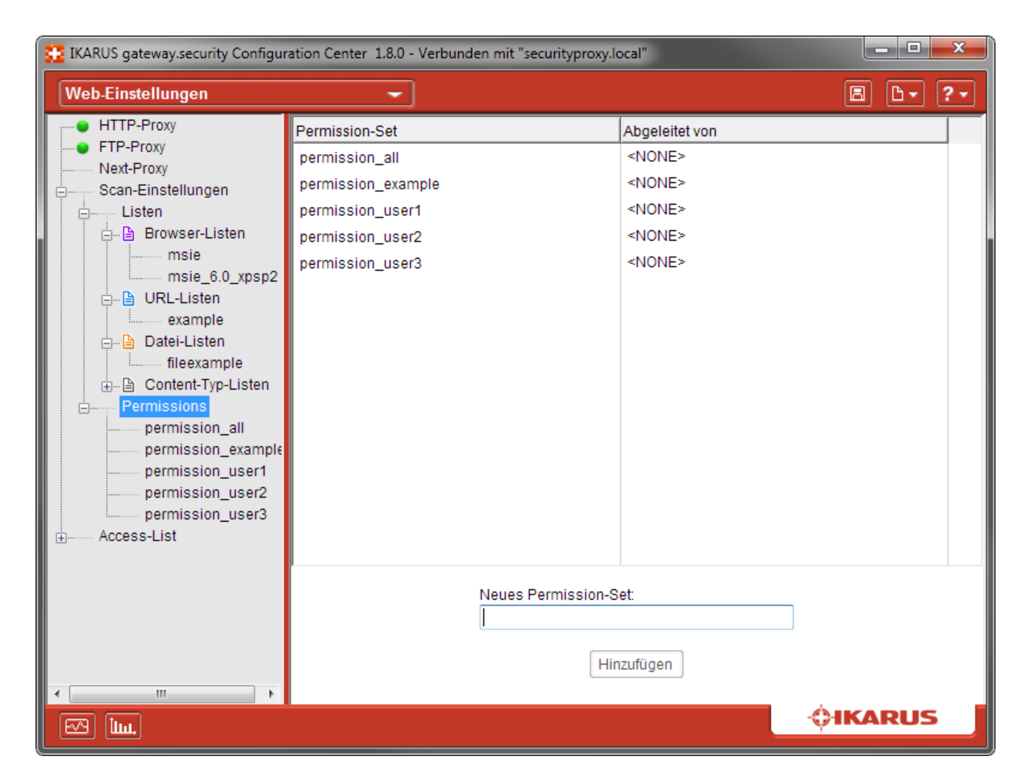


Abbildung 68: Userspezifische Permission-Sets

Der passende Eintrag in der Access-Liste wäre:

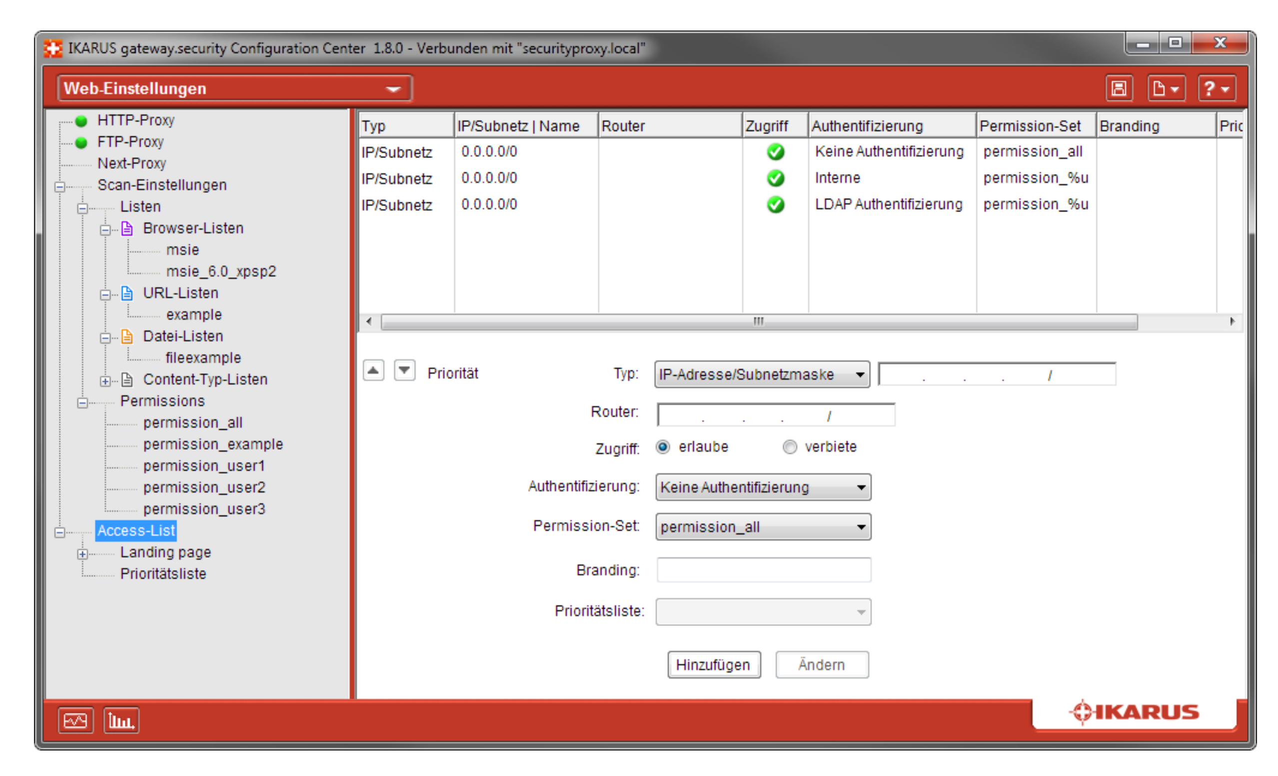


Abbildung 69: Eintrag userspezifischer Permission-Sets in Access-List

1. Bei „Proxy-interner Authentifizierung“, sprich wenn Sie für die Permission-Sets Passwörter definiert haben (**IKARUS gateway.security** Userverwaltung).

2. Bei „LDAP Authentifizierung“, wenn Sie ein Active Directory oder vergleichbares verwenden wollen (Domänenuser und Passwort).

3. Bei „NTLM/Kerberos Authentifizierung“, wenn Sie ein Active Directory oder vergleichbares verwenden wollen (Kerberos-Tickets).

Das %u in der Spalte „Permission-Set“ wird durch den jeweiligen Usernamen ersetzt.

4.9 Das Reporting

IKARUS gateway.security bietet die Möglichkeit, Ihre Aktivitäten im Bereich Mail und Web auszuwerten. Hierfür können Sie im **IKARUS gateway.security Configuration Center** Reports erstellen und anzeigen lassen und das Backend konfigurieren, sodass Reports automatisch generiert und verschickt werden.

4.9.1 Report erstellen

1. Öffnen Sie das **IKARUS gateway.security Configuration Center** und wählen Sie in der Menü-Auswahl links den Punkt ”Reporting”.

2. Hier wählen Sie den Punkt „Definierte Reports“ und anschließend eine Vorlage aus der Liste. Diese Vorlage bildet die Basis Ihres Reports. In der Vorschaubox unten auf der Seite können Sie sich bereits ansehen, was die Standardeinstellungen dieser Vorlage sind.

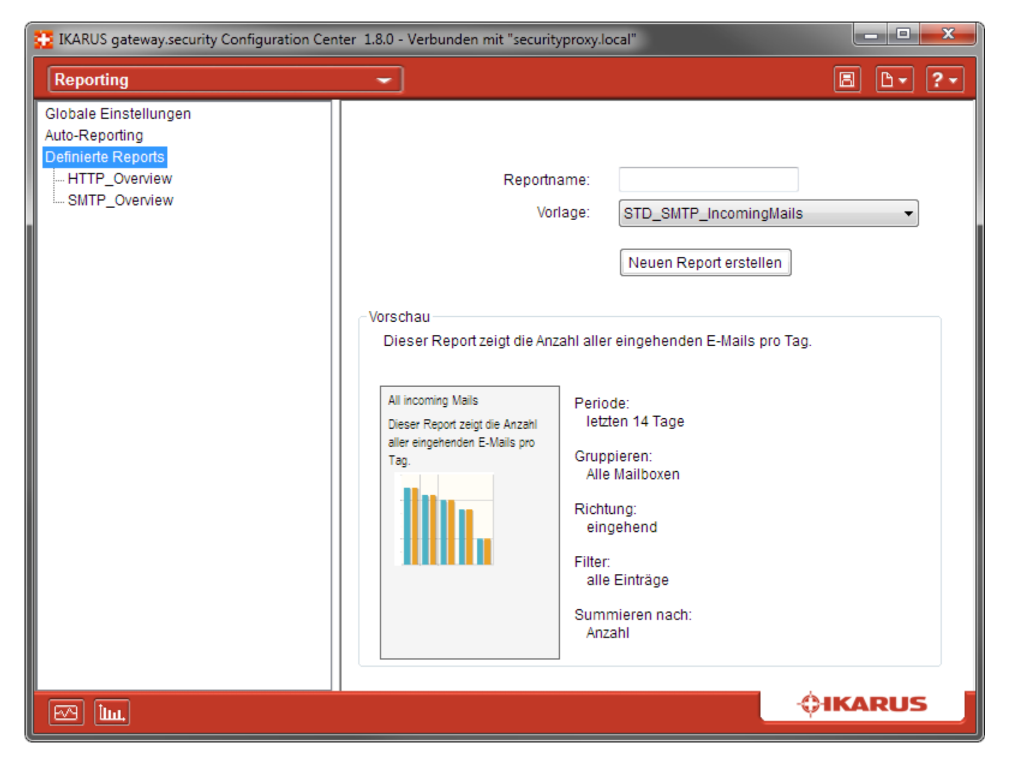


Abbildung 70: Reporting: neuer Report

3. Wählen Sie nun einen Namen für den neuen Report und klicken Sie den Button „Neuen Report erstellen“.

4.9.2 Report bearbeiten

1. Wählen Sie den zu bearbeitenden Report im Baum links aus.

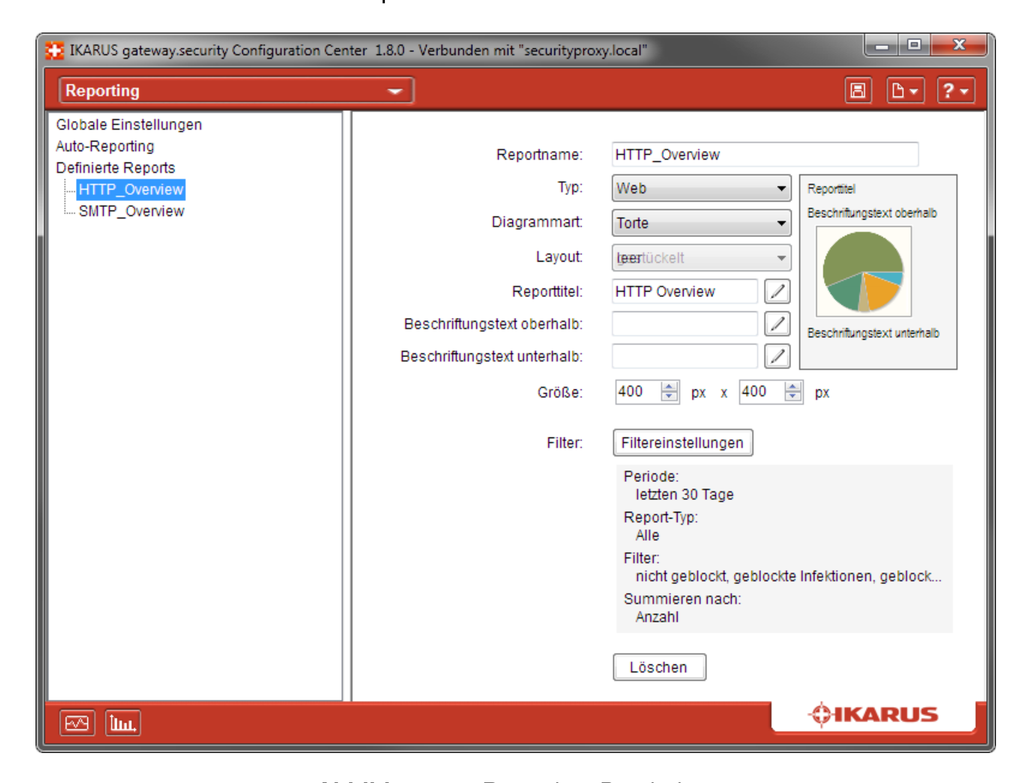


Abbildung 71: Reporting: Bearbeiten

2. Sie erhalten rechts die allgemeinen Einstellungen des Reports. Hier können Sie folgendes einstellen:
    - den Typ des Reports
    - die Dargestellung der Daten (Balken-, Torten- oder Liniendiagramm)
    - den Titel des Reports und evtl. Erklärungs- oder Ergänzungstexte
    - die Größe des Diagramms
3. Mit den jeweiligen Filtereinstellungen können Sie nun bestimmen was der Report genau zeigen soll. (Felderklärung siehe Kapitel Reporting)
4. Speichern Sie nun Ihren bearbeiteten Report.

4.9.3 Report anzeigen

Öffnen Sie den Reporting-Anzeige-Dialog.



Hier können Sie in der Liste Ihren gewünschten Report auswählen und mit einem „Klick“ auf den Button „Report anzeigen“ wird der Report generiert und in dem mittleren Bereich angezeigt.

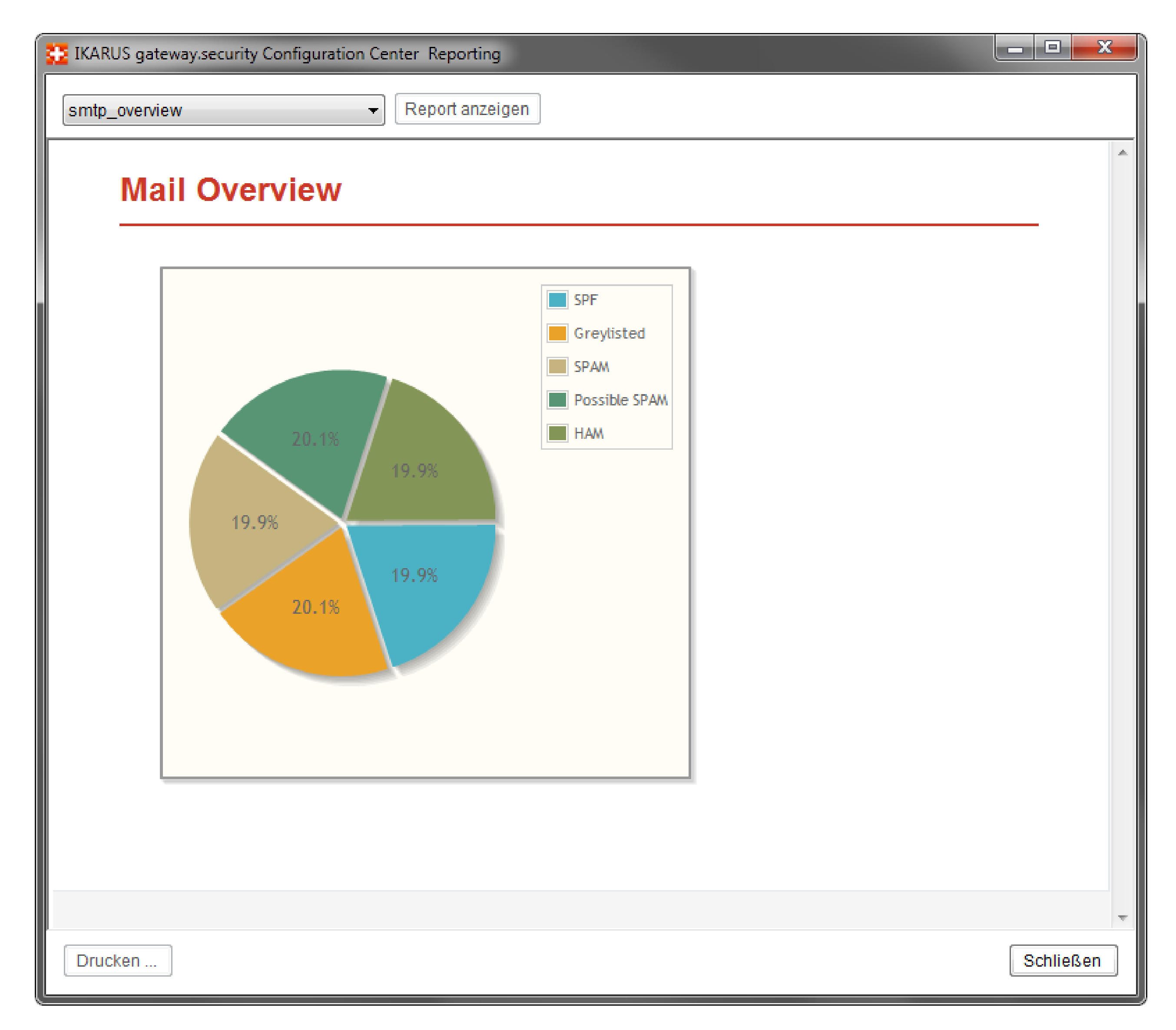


Abbildung 72: Reporting: Anzeigen

4.9.4 Report automatisch verschicken

Wählen Sie den Punkt „Auto-Reporting“ in der Baumansicht. Hier können Sie definieren, welche Reports Sie zu welchem Zeitpunkt wohin geschickt bekommen wollen.

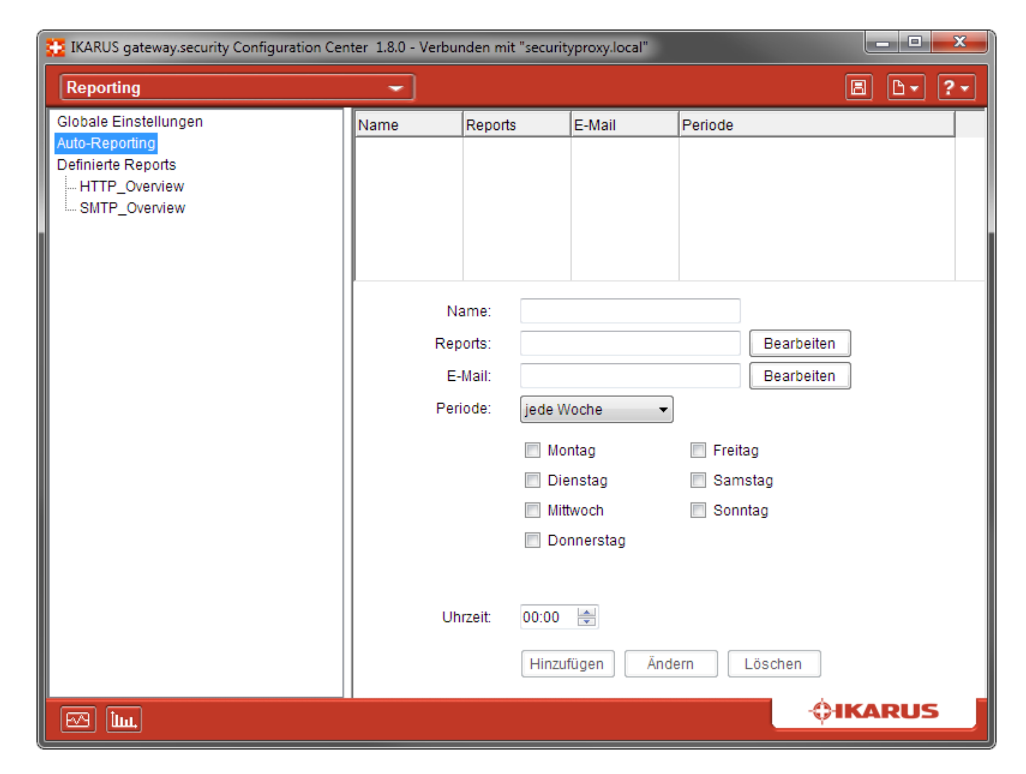


Abbildung 73: Reporting: Auto-Reporting

1. Zuerst geben Sie dem Auto-Reporting-Eintrag einen Namen.
2. Anschließend wählen Sie mit Hilfe des Bearbeiten-Buttons die Reports aus, die automatisch erstellt werden sollen.
3. Danach geben Sie den oder die Empfänger des automatisiert erstellten HTML-Reports über die E-Mail-Bearbeiten-Schaltfläche an.
4. Im nächsten Schritt selektieren Sie die Tage der Woche oder die Tage des Monats, an denen die ausgewählten Reports als E-Mail verschickt werden sollen.
5. Darüberhinaus bestimmen Sie noch die Uhrzeit, zu der die ausgewählten Reports automatisch erstellt und gesendet werden. Hierfür eignet sich eine Zeit, zu der **IKARUS gateway.security** nicht stark ausgelastet ist.
6. Abschließend fügen Sie den Eintrag über die Schaltfläche „Hinzufügen“ hinzu und speichern die neue Konfiguration. Ab jetzt werden die ausgewählten Reports zu einer gewissen Zeit an bestimmten Tagen erstellt und an die angebenen Empfänger geschickt.



5 IKARUS gateway.security FAQ

- ***IKARUS gateway.security lässt sich unter Microsoft Windows/Linux nicht installieren.***
  Geben Sie Acht, dass Sie das richtige Setup für die Plattform verwenden. Sie benötigen für die Installation entsprechende administrative Rechte auf Ihrem System. **IKARUS** stellt sowohl für Microsoft Windows als auch für Linux **gateway.security** Setups für 32 bit und 64 bit zur Verfügung. Für Linux existieren Installationspakete im `*.deb` und `*.rpm` Format.

- ***Es ist nicht möglich, eine Verbindung mit der Management-Konsole zu IKARUS gateway.security aufzubauen.***
  Ist das Service **IKARUS gateway.security** gestartet? Sind die TCP Ports gebunden? Standard für HTTP 8080, Remote-Management 15639. Wird der Zugriff evtl. von einer Firewall geblockt?

- ***Nach dem Start des Services von IKARUS gateway.security ist keine Funktion festzustellen.***
  Vergewissern Sie sich, ob das Service wirklich fehlerfrei gestartet werden konnte. Alle Informationen dazu finden Sie im Logfile `splogfile.log`, welches sich im „log“-Verzeichnis von **IKARUS gateway.security** befindet. Falls Sie **IKARUS gateway.security** auf einem System installieren, welches bereits andere Dienste zur Verfügung stellt (z.B. andere Proxys, andere Mail-Relay Agenten), kann es durchaus zu einer Port-„Kollision“ kommen. D.h. ein TCP-Port, welches **IKARUS gateway.security** nach der Installation definiert hat (oder eines definiert wurde) kollidiert mit einem bereits verwendeten. Folglich kann der Dienst von **IKARUS gateway.security** nicht an dem TCP-Port gebunden werden. Genau diese Fehlermeldungen finden Sie im oben angeführten Logfile.

- ***IKARUS gateway.security kann keine Updates durchführen bzw. erhalten. „Surfen“ über den Proxy ist auch nicht möglich.***
  Je nach Konfiguration von **IKARUS gateway.security** benötigt dieser entsprechenden Zugriff ins Internet, da dieser als „Proxy“ stellvertretend Inhalte aus dem Internet abruft. Auch das Abrufen der Updates erfolgt über diesen Weg – genauer gesagt über HTTP. Darum ist es wichtig, dass der Server mit folgenden Protokollen an einer Firewall freigeschaltet wird. Achtung: Aus Kundensicht „von innen nach außen“!!! Hier die vollständige Liste für die Applikation: HTTP, FTP, HTTPS, POP3, IMAP, NNTP. Es bedarf u.a. einer anderen wichtigen Konfiguration des Betriebssystems VOR der Installation von **IKARUS gateway.security**. Und zwar benötigt das System definierte DNS-Server. Somit muss das System auch für DNS-Abfragen an der Firewall freigeschaltet werden.

- ***Beim Aufruf einer Web-Seite erfolgt eine Meldung, dass die Lizenz abgelaufen oder ungültig ist.***
  Die Lizenz ist abgelaufen oder noch gar nicht hinzugefügt worden. Fügen Sie die Lizenz mit der Management Console oder per Kommandozeile hinzu.

- ***Wie stellt man sicher, dass man beim Zugriff auf Internet-Inhalte IKARUS gateway.security verwendet und somit mittels Gateway-Virenschutz surft?***
  Im jeweilig eingesetzten Web-Client (z.B. Microsoft Internet Explorer, Mozilla Firefox, Opera, Google Chrome, Safari) sind die Proxy Einstellungen vorzunehmen. Da es sich um einen Web-Client handelt, ist dafür immer das Port des HTTP-Proxy-Teils von **IKARUS gateway.security** zu verwenden.

- ***Kann man über IKARUS gateway.security auch verschlüsselte Seiten (via https://) abrufen?***
  Ja. Auch hier muss das Port des HTTP-Proxy verwendet werden. **IKARUS gateway.security** tunnelt den HTTPS Datenstrom zum Zielsystem. Da es sich um eine verschlüsselte Verbindung zwischen Client und Server handelt, erfolgt in diesem Fall kein Content-Filtering und somit auch kein Virenschutz. Es ist dafür Sorge zu tragen, dass am Client selbst nach wie vor ein lokaler Virenschutz vorhanden ist. **IKARUS** bietet auch hier eine Endpoint Protection Lösung an: **IKARUS anti.virus**.



- ***Kann verschlüsselter Datenverkehr (via https://) auf gefährlichen Inhalt überprüft werden?***
  Ohne zusätzliche Konfiguration und ohne Einsatz einer optional erhältlichen Software ist dies nicht möglich. Bitte wenden Sie sich an **IKARUS**, falls sie https absichern möchten.

- ***Kann man problemlos auf einen FTP-Server mit dem Microsoft Internet Explorer zugreifen?***
  Ja. Stellen Sie fest, dass Sie in den Proxy-Einstellungen des Microsoft Internet Explorer den „HTTP"-Proxy Teil von **IKARUS gateway.security** definiert haben – und zwar auch unter „ftp". Greifen Sie nun auf den FTP-Server über einen FTP-Link zu (z.B. ftp://ftp.example.org/). Kurz darauf werden Sie ggf. zur Authentifizierung gegenüber dem FTP-Server aufgefordert – sofern Sie dafür Benutzernamen und Passwort benötigen.

- ***Kann man das Passwort für den ROOT-Benutzer wieder zurücksetzen?***
  Ja. Die Passworte werden verschlüsselt auf dem **IKARUS gateway.security**-Server in der Datei `conf passwd` abgelegt. Wird in dieser Datei die Zeile beginnend mit `root:` gelöscht, so kann sich der Benutzer "root" wieder mit dem Standard-Passwort "root" anmelden. **Wichtig:** Es liegt in der Verantwortung des Systemadministrators, den Zugriff auf das Dateisystem des Servers hinreichend einzuschränken. Nach dem Zurücksetzen des Passworts muss es sobald wie möglich wieder geändert werden.



6 Glossar

Begriff	Erklärung
IKARUS AntiSPAM Engine	Die **IKARUS** AntiSPAM Engine überprüft den übermittelten Inhalt mit den Informationen aus der AntiSPAM Datenbank auf SPAM.
AntiSPAM Datenbank (SDB)	Die AntiSPAM-Datenbank wird vom Hersteller **IKARUS** automatisiert an SIS Scan Center zur Verfügung gestellt und dient der **IKARUS** AntiSPAM Engine als Basis zur Differenzierung zwischen SPAM und nicht SPAM.
IKARUS Scan Engine	**IKARUS** Scan Engine überprüft übermittelten Inhalt auf gefährlichen Inhalt.
Virendatenbank (VDB)	Die Virendatenbank dient der **IKARUS** Scan Engine als Informationsquelle für bekannte Malware.
Proxy	Ein Zwischenservice, das Anfragen von Clients entgegennimmt und an externe Ressourcen weiterleitet
SSL	Secure Socket Layer
HTTP	Hyper Text Transfer Protocol
FTP	File Transfer Protocol
HTTPS	Hyper Text Transfer Protocol mit SSL Verschlüsselung
SMTP	Simple Mail Transfer Protocol
POP3	Post Office Protocol version 3
IMAP	Internet Message Access Protocol
NNTP	Network News Transfer Protocol

Tabelle 40: Glossar

IKARUS Security Software GmbH · Blechturmgasse 11 · 1050 Vienna · Austria